

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2018-50107

(P2018-50107A)

(43) 公開日 平成30年3月29日 (2018. 3. 29)

(51) Int.Cl.	F I	テーマコード (参考)
HO4L 9/08 (2006.01)	HO4L 9/00 601A	5J104
GO6F 21/62 (2013.01)	HO4L 9/00 601E	
	GO6F 21/62 318	

審査請求 未請求 請求項の数 21 O L (全 33 頁)

(21) 出願番号 特願2016-182831 (P2016-182831)
 (22) 出願日 平成28年9月20日 (2016. 9. 20)

(71) 出願人 000001270
 コニカミノルタ株式会社
 東京都千代田区丸の内二丁目7番2号
 (74) 代理人 100117651
 弁理士 高垣 泰志
 (72) 発明者 山口 敏伸
 東京都千代田区丸の内二丁目7番2号 コ
 ニカミノルタ株式会社内
 Fターム(参考) 5J104 AA16 EA15 EA16 EA18 EA19
 NA02 NA05 NA37 PA14

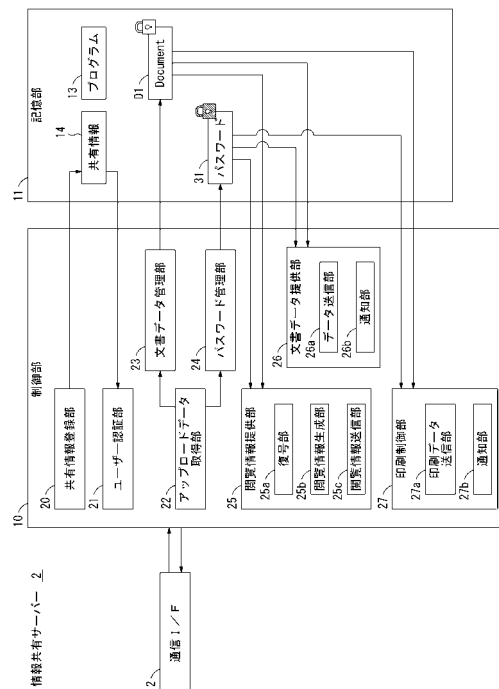
(54) 【発明の名称】 情報共有サーバー、情報共有システム及びプログラム

(57) 【要約】

【課題】パスワードによって暗号化された文書データがアップロードされた場合において他のユーザーがパスワードを知らなくても文書データを閲覧できるようにする。

【解決手段】情報共有サーバー2は、文書データD1を共有する複数のユーザーを一のグループに登録する共有情報登録部20と、一のグループに含まれる一のユーザーによって暗号化された文書データD1と、文書データD1を復号するためのパスワードとを取得する取得部22と、暗号化された文書データD1と、パスワードとを関連付けて記憶する記憶部11と、一のグループに含まれるいずれかのユーザーから文書データD1の閲覧要求を受け付けた場合に、記憶部11から文書データD1とパスワードとを読み出し、パスワードを用いて暗号化された文書データD1を復号する復号部25aと、復号された文書データD1を、閲覧要求の送信元に対して提供する閲覧情報提供部25と、を備える。

【選択図】 図4



【特許請求の範囲】**【請求項 1】**

文書データを共有する複数のユーザーを一のグループに登録する登録手段と、
前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する取得手段と、
前記暗号化された文書データと、前記パスワードとを関連付けて記憶する記憶手段と、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記記憶手段から前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する復号手段と、

10

前記復号手段によって復号された文書データを、前記閲覧要求の送信元に対して提供する閲覧情報提供手段と、
を備えることを特徴とする情報共有サーバー。

【請求項 2】

前記閲覧情報提供手段は、前記復号された文書データに基づいて閲覧用画像を生成し、前記閲覧要求の送信元に対して前記閲覧用画像を送信することを特徴とする請求項 1 に記載の情報共有サーバー。

【請求項 3】

前記登録手段は、前記一のグループに対して一対の暗号鍵と復号鍵を登録し、
前記記憶手段は、前記パスワードが前記暗号鍵によって暗号化された暗号化パスワードを記憶し、
前記復号化手段は、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする請求項 1 又は 2 に記載の情報共有サーバー。

20

【請求項 4】

前記取得手段は、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする請求項 3 に記載の情報共有サーバー。

【請求項 5】

前記取得手段は、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする請求項 3 に記載の情報共有サーバー。

30

【請求項 6】

前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記記憶手段には、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第 1 の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第 2 の暗号化パスワードとが記憶されることを特徴とする請求項 3 乃至 5 のいずれかに記載の情報共有サーバー。

40

【請求項 7】

前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する文書データ送信手段、
を更に備えることを特徴とする請求項 1 乃至 6 のいずれかに記載の情報共有サーバー。

【請求項 8】

前記文書データ送信手段により前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する通知手段、
を更に備えることを特徴とする請求項 7 に記載の情報共有サーバー。

50

【請求項 9】

前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記印刷要求で指定された印刷装置へ送信する印刷制御手段、
を更に備えることを特徴とする請求項 1 乃至 8 のいずれかに記載の情報共有サーバー。

【請求項 10】

請求項 1 乃至 9 のいずれかに記載の情報共有サーバーと、
前記情報共有サーバーに対して文書データをアップロードする情報処理装置と、
を有する情報共有システムであって、
前記情報処理装置は、
文書データをユーザーによって指定されたパスワードで暗号化する暗号化手段と、
前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、
を備えることを特徴とする情報共有システム。

10

【請求項 11】

請求項 1 乃至 9 のいずれかに記載の情報共有サーバーと、
前記情報共有サーバーに対して文書データをアップロードする画像処理装置と、
を有する情報共有システムであって、
前記画像処理装置は、
原稿を読み取ることによって文書データを生成する原稿読取手段と、
前記原稿読取手段によって生成された文書データを、ユーザーによって指定されたパスワードで暗号化する暗号化手段と、
前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、
を備えることを特徴とする情報共有システム。

20

【請求項 12】

前記アップロード手段は、前記暗号化された文書データを前記情報共有サーバーへアップロードすることに伴い、前記情報共有サーバーから暗号鍵を受信した場合、前記暗号鍵を用いて前記パスワードを暗号化した暗号化パスワードを生成し、前記暗号化パスワードを前記情報共有サーバーへアップロードすることを特徴とする請求項 10 又は 11 に記載の情報共有システム。

30

【請求項 13】

コンピュータに、
文書データを共有する複数のユーザーを一のグループに登録する第 1 ステップと、
前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する第 2 ステップと、
前記暗号化された文書データと、前記パスワードとを関連付けて記憶する第 3 ステップと、
前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを読み出し、
前記パスワードを用いて前記暗号化された文書データを復号する第 4 ステップと、
前記第 4 ステップによって復号された文書データを、前記閲覧要求の送信元に対して提供する第 5 ステップと、
を実行させることを特徴とするプログラム。

40

【請求項 14】

前記第 5 ステップは、前記復号された文書データに基づいて閲覧用画像を生成し、前記閲覧要求の送信元に対して前記閲覧用画像を送信することを特徴とする請求項 13 に記載のプログラム。

【請求項 15】

前記第 1 ステップは、前記一のグループに対して一対の暗号鍵と復号鍵を登録するステ

50

ップを含み、

前記第3ステップは、前記暗号鍵によって前記パスワードが暗号化された暗号化パスワードを記憶し、

前記第4ステップは、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする請求項13又は14に記載のプログラム。

【請求項16】

前記第2ステップは、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする請求項15に記載のプログラム。

【請求項17】

前記第2ステップは、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする請求項15に記載のプログラム。

【請求項18】

前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記第3ステップは、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第1の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第2の暗号化パスワードとを記憶することを特徴とする請求項15乃至17のいずれかに記載のプログラム。

【請求項19】

前記コンピュータに、

前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する第6ステップ、
を更に実行させることを特徴とする請求項13乃至18のいずれかに記載のプログラム。

【請求項20】

前記コンピュータに、

前記第6ステップにより前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する第7ステップ、
を更に実行させることを特徴とする請求項19に記載のプログラム。

【請求項21】

前記コンピュータに、

前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記印刷要求で指定された印刷装置へ送信する第8ステップ、
を更に実行させることを特徴とする請求項13乃至20のいずれかに記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報共有サーバー、情報共有システム及びプログラムに関し、特に複数のユーザーで文書データを共有するための技術に関する。

【背景技術】

【0002】

従来、インターネットに接続されたクラウド上にWebサーバーとして機能する情報共有サーバーを設置し、複数のユーザーがそれぞれ異なる拠点から情報共有サーバーへアクセスしてログインすることにより、複数のユーザーが情報を共有しながら会議などを行え

10

20

30

40

50

るようにした情報共有サービスが提供されている。この種の情報共有サービスでは、各ユーザーが作成した文書データを情報共有サーバーへアップロードすることにより、複数のユーザーがその文書データを共有することも可能である。

【0003】

また情報共有サーバーは、アップロードされる文書データを、予め登録された複数のユーザー以外には公開しない機能を有している。そのため、情報共有サーバーには、パスワードによって暗号化された機密性の高い文書データがアップロードされることもある（例えば特許文献1）。この場合、情報共有サーバーは、パスワードによって暗号化された文書データを共有情報として保存することとなる。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2014-174721号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、情報共有サーバーにおいて保存される文書データに設定されたパスワードが文書データ毎に異なる場合、各ユーザーは個々の文書データに設定されているパスワードを自身で入力しなければ文書データの中身を閲覧することができない。そのため、文書データをアップロードするユーザーは、文書データに設定したパスワードを他のユーザーに通知する必要があり、煩わしい。

【0006】

一方、文書データをアップロードしたユーザーがその文書データを閲覧する際の画面情報を他のユーザーにも提供できるように構成すれば、他のユーザーは文書データのパスワードを知らなくても、文書データの中身を閲覧することができる。しかし、このような構成では、他のユーザーは、文書データをアップロードしたユーザーがその文書データを閲覧しているときにしか閲覧できないため、利便性に欠けるという問題がある。

【0007】

また文書データをアップロードするユーザーによって任意のパスワードが設定されると、情報共有サーバーは、そのパスワードを把握することができないため、他のユーザーに対し、パスワードによって暗号化された文書データのプレビュー機能を提供することができないという問題もある。

【0008】

これに対し、文書データをアップロードするユーザーが、パスワードを設定することなく、文書データを文書共有サーバーへアップロードすれば、上記のような問題は解消される。しかし、この場合、他のユーザーによって文書データがダウンロードされてしまうと、文書データの閲覧に関する制限を課すことができなくなるため、情報漏洩のリスクが高くなるという新たな問題が発生する。

【0009】

そこで本発明は、上記問題点を解決するためになされたものであり、パスワードによって暗号化された文書データがアップロードされた場合に、他のユーザーがパスワードを知らなくても文書データを閲覧できるようにして利便性を向上させた情報共有サーバー、情報共有システム及びプログラムを提供することを目的とする。

【課題を解決するための手段】

【0010】

上記目的を達成するため、請求項1に係る発明は、情報共有サーバーであって、文書データを共有する複数のユーザーを一のグループに登録する登録手段と、前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する取得手段と、前記暗号化された文書データと、前記パスワードとを関連付けて記憶する記憶手段と、前記一のグループに含まれるい

10

20

30

40

50

れかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記記憶手段から前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する復号手段と、前記復号手段によって復号された文書データを、前記閲覧要求の送信元に対して提供する閲覧情報提供手段と、を備えることを特徴とする構成である。

【0011】

請求項2に係る発明は、請求項1に記載の情報共有サーバーにおいて、前記閲覧情報提供手段は、前記復号された文書データに基づいて閲覧用画像を生成し、前記閲覧要求の送信元に対して前記閲覧用画像を送信することを特徴とする構成である。

【0012】

請求項3に係る発明は、請求項1又は2に記載の情報共有サーバーにおいて、前記登録手段は、前記一のグループに対して一対の暗号鍵と復号鍵を登録し、前記記憶手段は、前記パスワードが前記暗号鍵によって暗号化された暗号化パスワードを記憶し、前記復号化手段は、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする構成である。

【0013】

請求項4に係る発明は、請求項3に記載の情報共有サーバーにおいて、前記取得手段は、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする構成である。

【0014】

請求項5に係る発明は、請求項3に記載の情報共有サーバーにおいて、前記取得手段は、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする構成である。

【0015】

請求項6に係る発明は、請求項3乃至5のいずれかに記載の情報共有サーバーにおいて、前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記記憶手段には、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第1の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第2の暗号化パスワードとが記憶されることを特徴とする構成である。

【0016】

請求項7に係る発明は、請求項1乃至6のいずれかに記載の情報共有サーバーにおいて、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する文書データ送信手段、を更に備えることを特徴とする構成である。

【0017】

請求項8に係る発明は、請求項7に記載の情報共有サーバーにおいて、前記文書データ送信手段により前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する通知手段、を更に備えることを特徴とする構成である。

【0018】

請求項9に係る発明は、請求項1乃至8のいずれかに記載の情報共有サーバーにおいて、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記印刷要求で指定された印刷装置へ送信する印刷制御手段、を更に備えることを特徴とする構成である。

10

20

30

40

50

【 0 0 1 9 】

請求項 1 0 に係る発明は、請求項 1 乃至 9 のいずれかに記載の情報共有サーバーと、前記情報共有サーバーに対して文書データをアップロードする情報処理装置と、を有する情報共有システムであって、前記情報処理装置は、文書データをユーザーによって指定されたパスワードで暗号化する暗号化手段と、前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、を備えることを特徴とする構成である。

【 0 0 2 0 】

請求項 1 1 に係る発明は、請求項 1 乃至 9 のいずれかに記載の情報共有サーバーと、前記情報共有サーバーに対して文書データをアップロードする画像処理装置と、を有する情報共有システムであって、前記画像処理装置は、原稿を読み取ることによって文書データを生成する原稿読取手段と、前記原稿読取手段によって生成された文書データを、ユーザーによって指定されたパスワードで暗号化する暗号化手段と、前記暗号化手段によって暗号化された文書データと前記パスワードとを前記情報共有サーバーへアップロードするアップロード手段と、を備えることを特徴とする構成である。

10

【 0 0 2 1 】

請求項 1 2 に係る発明は、請求項 1 0 又は 1 1 に記載の情報共有システムにおいて、前記アップロード手段は、前記暗号化された文書データを前記情報共有サーバーへアップロードすることに伴い、前記情報共有サーバーから暗号鍵を受信した場合、前記暗号鍵を用いて前記パスワードを暗号化した暗号化パスワードを生成し、前記暗号化パスワードを前記情報共有サーバーへアップロードすることを特徴とする構成である。

20

【 0 0 2 2 】

請求項 1 3 に係る発明は、プログラムであって、コンピュータに、文書データを共有する複数のユーザーを一のグループに登録する第 1 ステップと、前記一のグループに含まれる一のユーザーによって暗号化された文書データと、前記暗号化された文書データを復号するためのパスワードとを取得する第 2 ステップと、前記暗号化された文書データと、前記パスワードとを関連付けて記憶する第 3 ステップと、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの閲覧要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを読み出し、前記パスワードを用いて前記暗号化された文書データを復号する第 4 ステップと、前記第 4 ステップによって復号された文書データを、前記閲覧要求の送信元に対して提供する第 5 ステップと、を実行させることを特徴とする構成である。

30

【 0 0 2 3 】

請求項 1 4 に係る発明は、請求項 1 3 に記載のプログラムにおいて、前記第 5 ステップは、前記復号された文書データに基づいて閲覧用画像を生成し、前記閲覧要求の送信元に対して前記閲覧用画像を送信することを特徴とする構成である。

【 0 0 2 4 】

請求項 1 5 に係る発明は、請求項 1 3 又は 1 4 に記載のプログラムにおいて、前記第 1 ステップは、前記一のグループに対して一対の暗号鍵と復号鍵を登録するステップを含み、前記第 3 ステップは、前記暗号鍵によって前記パスワードが暗号化された暗号化パスワードを記憶し、前記第 4 ステップは、前記暗号化された文書データを復号する際、前記復号鍵を用いて前記暗号化パスワードから前記パスワードを復号することを特徴とする構成である。

40

【 0 0 2 5 】

請求項 1 6 に係る発明は、請求項 1 5 に記載のプログラムにおいて、前記第 2 ステップは、前記パスワードを取得した場合に、前記暗号鍵を用いて前記パスワードを暗号化して前記暗号化パスワードを生成することを特徴とする構成である。

【 0 0 2 6 】

請求項 1 7 に係る発明は、請求項 1 5 に記載のプログラムにおいて、前記第 2 ステップは、前記暗号化された文書データの送信元に対して前記暗号鍵を送信することにより、前

50

記暗号化された文書データの送信元において前記パスワードを暗号化させ、前記暗号化された文書データの送信元から前記暗号化パスワードを取得することを特徴とする構成である。

【0027】

請求項18に係る発明は、請求項15乃至17のいずれかに記載のプログラムにおいて、前記一のユーザーが前記一のグループとは異なる他のグループにも登録されており、前記一のユーザーが前記一のグループと前記他のグループとの双方で前記暗号化された文書データを共有することを指定した場合、前記第3ステップは、前記一のグループに登録されている暗号鍵で前記パスワードが暗号化された第1の暗号化パスワードと、前記他のグループに登録されている暗号鍵で前記パスワードが暗号化された第2の暗号化パスワードとを記憶することを特徴とする構成である。

10

【0028】

請求項19に係る発明は、請求項13乃至18のいずれかに記載のプログラムにおいて、前記コンピュータに、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データのダウンロード要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記ダウンロード要求の送信元へ送信する第6ステップ、を更に実行させることを特徴とする構成である。

【0029】

請求項20に係る発明は、請求項19に記載のプログラムにおいて、前記コンピュータに、前記第6ステップにより前記暗号化された文書データと前記パスワードとの送信が行われた場合に、前記ダウンロード要求を行ったユーザーに関する情報を前記一のユーザーに通知する第7ステップ、を更に実行させることを特徴とする構成である。

20

【0030】

請求項21に係る発明は、請求項13乃至20のいずれかに記載のプログラムにおいて、前記コンピュータに、前記一のグループに含まれるいずれかのユーザーから前記暗号化された文書データの印刷要求を受け付けた場合に、前記暗号化された文書データと前記パスワードとを前記印刷要求で指定された印刷装置へ送信する第8ステップ、を更に実行させることを特徴とする構成である。

【発明の効果】

【0031】

本発明によれば、パスワードによって暗号化された文書データがアップロードされた場合において、他のユーザーがパスワードを知らなくても文書データを閲覧することが可能になるため、暗号化された文書データを利用する際の利便性が向上する。

30

【図面の簡単な説明】

【0032】

【図1】情報共有システムの概念的構成例を示す図である。

【図2】情報処理装置のハードウェア構成及び機能構成の一例を示すブロック図である。

【図3】画像処理装置のハードウェア構成及び機能構成の一例を示すブロック図である。

【図4】情報共有サーバーのハードウェア構成及び機能構成の一例を示すブロック図である。

40

【図5】共有情報の一例を示す図である。

【図6】アップロードデータ取得部による暗号化処理の概念を示す図である。

【図7】管理情報の一例を示す図である。

【図8】復号部の詳細な機能構成の一例を示す図である。

【図9】閲覧情報生成部の詳細な機能構成の一例を示す図である。

【図10】情報処理装置において表示される閲覧画面の一例を示す図である。

【図11】文書データを情報共有サーバーへアップロードして閲覧する場合の動作シーケンスを示す図である。

【図12】文書データをダウンロードする場合の動作シーケンスを示す図である。

【図13】文書データを印刷する場合の動作シーケンスを示す図である。

50

【図14】情報共有サーバーによって行われる主たる処理手順の一例を示すフローチャートである。

【図15】文書データ登録処理の詳細な処理手順の一例を示すフローチャートである。

【図16】閲覧情報提供処理の詳細な処理手順の一例を示すフローチャートである。

【図17】文書データ提供処理の詳細な処理手順の一例を示すフローチャートである。

【図18】印刷制御処理の詳細な処理手順の一例を示すフローチャートである。

【図19】文書データを情報共有サーバーへアップロードする際の動作シーケンスを示す図である。

【発明を実施するための形態】

【0033】

10

以下、本発明に関する好ましい実施形態について図面を参照しつつ詳細に説明する。尚、以下に説明する実施形態において互いに共通する部材には同一符号を付しており、それらについての重複する説明は省略する。

【0034】

(第1実施形態)

図1は、本発明における情報共有システム1の概念的構成例を示す図である。情報共有システム1は、インターネットに接続されたクラウド3上に設けられる情報共有サーバー2と、複数の情報処理装置4と、スキャン機能及びプリント機能を備えたMFP(Multifunction Peripherals)などで構成される画像処理装置5とが、インターネットなどのネットワークを介して相互にデータ通信を行うことができる構成である。複数の情報処理装置4のそれぞれは、例えば一般的なパーソナルコンピュータ(PC)によって構成される。各情報処理装置4は、それぞれ異なるユーザーA, B, C, Dによって使用される。またユーザーA, B, C, Dは、例えばそれぞれ異なる拠点に位置している。画像処理装置5は、例えばユーザーAと同じ拠点に設置されており、ユーザーAが使用可能である。

20

【0035】

情報共有サーバー2は、Webサーバー機能、情報共有機能、TV会議機能などの様々な機能を備えており、予め登録された複数のユーザーA, B, C, Dが同じ情報を共有することができる情報共有サービスを提供する。例えば、情報共有サーバー2は、ユーザーAが操作する情報処理装置4から文書データD1がアップロードされると、その文書データD1を保存して管理する。そして他のユーザーB, C, Dからその文書データD1の閲覧要求を受信すると、情報共有サーバー2は、ユーザーAによってアップロードされた文書データD1を他のユーザーB, C, Dに公開する。

30

【0036】

文書データD1をアップロードするとき、文書データD1が機密性の高い文書であれば、ユーザーAは、情報処理装置4を操作することにより、文書データD1に対して任意のパスワードを設定し、文書データD1を暗号化する。そしてユーザーAは、自身が設定したパスワードで暗号化された文書データD1を情報共有サーバー2へアップロードする。このとき、情報処理装置4は、暗号された文書データD1と共に、文書データD1を復号するためのパスワード(ユーザーAによって設定されたパスワード)を情報共有サーバー2へ送信する。

40

【0037】

この他にも、ユーザーAは、画像処理装置5のスキャン機能を利用して原稿9を読み取って生成された文書データD1を情報共有サーバー2へアップロードすることもできる。この場合、画像処理装置5で生成される文書データD1を、ユーザーAの情報処理装置4へ一旦転送した後、ユーザーAの情報処理装置4から情報共有サーバー2へアップロードする第1の手法と、画像処理装置5で生成される文書データD1を、画像処理装置5から情報共有サーバー2へ直接アップロードする第2の手法とがある。第1の手法の場合、ユーザーAがパスワードを設定して文書データD1を暗号化する処理は、画像処理装置5と情報処理装置4のいずれで行っても良い。これに対し、第2の手法の場合、画像処理装置5は、ユーザーAによるパスワードの設定操作を受け付け、原稿9を読み取って生成した

50

文書データD1を暗号化し、暗号化された文書データD1と共に、ユーザーAによって設定されたパスワードを情報共有サーバー2へ送信する。

【0038】

情報共有サーバー2は、ユーザーAの情報処理装置4又は画像処理装置5から、暗号化された文書データD1と、パスワードと、を受信すると、それらを相互に関連付けた状態で記憶する。そして情報共有サーバー2は、ユーザーAによってアップロードされた文書データD1を、予め登録された複数のユーザーA、B、C、Dによる共有対象の文書データとして管理する。

【0039】

他のユーザーB、C、DがユーザーAによってアップロードされた文書データD1を閲覧するとき、各ユーザーB、C、Dは、自身の情報処理装置4を操作することによって情報共有サーバー2にアクセスし、情報共有サーバー2にログインする。そして各ユーザーB、C、Dは、ユーザーAによってアップロードされた文書データD1の閲覧要求を情報共有サーバー2へ送信する。

10

【0040】

情報共有サーバー2は、他のユーザーB、C、Dからの閲覧要求を受信すると、ユーザーAによってアップロードされた暗号化された文書データD1とパスワードとを読み出す。そしてユーザーAによって設定されたパスワードを用いて暗号化された文書データD1を復号し、他のユーザーB、C、Dが閲覧可能な文書データD2を生成する。その後、情報共有サーバー2は、復号した文書データD2に基づく閲覧画面を生成し、他のユーザーB、C、Dの情報処理装置4へ送信する。これにより、他のユーザーB、C、Dは、ユーザーAによって文書データD1に設定されたパスワードを知らなくても、文書データD1の中身を閲覧することができるようになる。以下、このような情報共有システム1について更に詳しく説明する。

20

【0041】

まず情報処理装置4について説明する。図2は、情報処理装置4のハードウェア構成及び機能構成の一例を示すブロック図である。情報処理装置4は、ハードウェア構成として、CPUやメモリなどを備えて構成される制御部40と、各種情報を記憶する記憶部41と、カラー液晶ディスプレイなどで構成される表示部42と、キーボードやマウス、タッチパネルなどで構成される操作部43と、情報共有サーバー2などの他の装置と通信を行うための通信インターフェース44とを備えている。

30

【0042】

記憶部41は、ハードディスクドライブ(HDD)やソリッドステートドライブ(SSD)などで構成される不揮発性の記憶手段である。この記憶部41には、制御部40のCPUによって実行されるアプリケーションプログラム45やブラウザプログラム46が記憶されている。アプリケーションプログラムは、情報処理装置4において文書データD1を作成する文書作成アプリケーション47を起動させるためのプログラムである。ブラウザプログラム46は、情報処理装置4においてWebページなどの閲覧画面を取得し、その閲覧画面を表示部42に表示するWebブラウザ48を起動させるためのプログラムである。また記憶部41には、情報共有サーバー2へのアップロード対象となる文書データD1を記憶することが可能である。

40

【0043】

文書作成アプリケーション47は、操作部43に対するユーザーの操作に基づいて文書の作成及び編集を行い、文書データD1を生成する処理部である。この文書作成アプリケーション47は、パスワード設定部51、文書データ暗号化部52及び文書データ保存部53を備えている。

【0044】

パスワード設定部51は、ユーザーの操作に基づいて作成した文書データD1を暗号化する際に機能し、パスワード設定画面を表示部42に表示し、ユーザーによって操作部43に入力されるパスワードを受け付ける。パスワード設定部51は、ユーザーによって指

50

定されたパスワードを文書データD1の暗号化用のパスワードに設定し、そのパスワードを文書データ暗号化部52へ出力する。

【0045】

文書データ暗号化部52は、パスワード設定部51によって設定されたパスワードを用いて文書データD1を暗号化する。これにより、文書データD1は、パスワードを入力しない限り、その内容を閲覧することができない暗号データに変換される。そして文書データ暗号化部52は、暗号化された文書データD1を文書データ保存部53へ出力する。

【0046】

文書データ保存部53は、暗号化された文書データD1を記憶部41に保存する。尚、ユーザーによって文書データD1の暗号化が指定されていない場合、文書データ保存部53は、暗号化されていない文書データD1を記憶部41へ保存することもできる。

10

【0047】

Webブラウザ48は、通信インタフェース44を介して、ユーザーによって指定されたURLのアドレスにアクセスし、そのアドレスにあるサーバーと通信を行い、サーバーから閲覧画面を取得して表示部42に表示したり、閲覧画面に対するユーザーの操作に基づく操作情報をサーバーへ送信したりする。Webブラウザ48は、閲覧表示部55と、アップロード部56とを備えている。閲覧表示部55は、サーバーから閲覧画面を取得して表示部42に表示させると共に、操作情報をサーバーへ送信するためのものであり、Webブラウザ48に標準搭載されている機能である。アップロード部56は、例えばサーバーから取得した閲覧画面に含まれるスクリプトプログラムなどをWebブラウザ48が実行することによって実現される機能であり、ユーザーによって指定された文書データD1をサーバーへアップロードする処理部である。

20

【0048】

例えばWebブラウザ48が情報共有サーバー2にアクセスし、情報共有サーバー2から取得した閲覧画面に含まれるスクリプトプログラムを実行することによってアップロード部56が機能した場合、アップロード部56は、ユーザーによって指定された文書データD1を情報共有サーバー2へアップロードする。またアップロード部56は、パスワードによって暗号化された文書データD1を情報共有サーバー2へアップロードするときには、暗号化された文書データD1と共に、文書データD1を復号するためのパスワードを情報共有サーバー2へアップロードする。そのため、アップロード部56は、暗号化された文書データD1を情報共有サーバー2へアップロードするとき、表示部42にパスワード入力画面を表示してユーザーによるパスワード入力操作を受け付ける。そしてユーザーによるパスワード入力操作が完了すると、アップロード部56は、ユーザーによって入力されたパスワードを、暗号化された文書データD1と共に情報共有サーバー2へアップロードする。

30

【0049】

したがって、情報処理装置4は、情報共有サーバー2に対して暗号化された文書データD1を送信するときには、暗号化された文書データD1だけでなく、その暗号化された文書データD1を復号するためのパスワードも同時に情報共有サーバー2へアップロードすることができる。

40

【0050】

次に画像処理装置5について説明する。図3は、画像処理装置5のハードウェア構成及び機能構成の一例を示すブロック図である。画像処理装置5は、ハードウェア構成として、CPUやメモリなどを備えて構成される制御部60と、各種情報を記憶する記憶部61と、ユーザーが画像処理装置5を使用する際のユーザーインタフェースとなる操作パネル62と、情報共有サーバー2などの他の装置と通信を行うための通信インタフェース63と、原稿の画像を光学的に読み取るスキャナ部64と、印刷出力を行うプリンタ部65とを備えている。また操作パネル62は、各種情報を表示する表示部62aと、ユーザーによる操作を受け付ける操作部62bとを備えている。記憶部61は、例えばハードディスクドライブ(HDD)によって構成される不揮発性の記憶手段である。この記憶部61に

50

は、制御部 40 の CPU によって実行されるプログラム 66 や、画像処理装置 5 を使用するユーザーに関する情報が登録されたユーザー情報 67 などが記憶される。

【0051】

制御部 60 の CPU は、画像処理装置 5 の起動時に記憶部 61 からプログラム 66 を自動的に読み出して実行する。これにより、制御部 60 は、ユーザー認証部 70、スキャンアプリケーション 71 及び印刷ジョブ実行部 72 として機能する。

【0052】

ユーザー認証部 70 は、画像処理装置 5 を使用するユーザーの認証処理を行う。例えばユーザー認証部 70 は、ユーザーが操作パネル 62 を操作することによって入力した情報がユーザー情報 67 に登録されているか否かを判別することにより、ユーザー認証を行う。ユーザーによって入力された情報がユーザー情報に登録されていれば、認証成功となるため、ユーザー認証部 70 は、画像処理装置 5 をユーザーが利用可能なログイン状態へ移行させる。これに対し、ユーザーによって入力された情報がユーザー情報に登録されていない場合、認証失敗となるため、ユーザーは画像処理装置 5 を利用することができない。

【0053】

スキャンアプリケーション 71 は、ユーザー認証に成功したログインユーザーがスキャン機能の利用を選択した場合に機能する。このスキャンアプリケーション 71 は、例えばユーザー情報 67 を参照し、画像処理装置 5 にログインしたユーザーが情報共有サーバー 2 を利用可能なユーザーであるか否かを判断する。その結果、ログインユーザーが情報共有サーバー 2 を利用可能なユーザーであれば、スキャン機能によって生成した文書データ D1 を情報共有サーバー 2 へアップロード可能な機能を動作させる。この場合、スキャンアプリケーション 71 は、原稿読取制御部 75、文書データ生成部 76、パスワード受付部 77、暗号化部 78 及びアップロード部 79 として機能する。

【0054】

原稿読取制御部 75 は、スキャナ部 64 に動作命令を出力することにより、ユーザーによってセットされた原稿 9 の読み取り動作を制御し、原稿 9 を読み取って生成されたデータを取得する。文書データ生成部 76 は、原稿読取制御部 75 が取得したデータを例えば PDF (Portable Document Format) などの所定のデータ形式に変換し、文書データ D1 を生成する。パスワード受付部 77 は、ユーザーによって文書データ D1 の暗号化が指定された場合に機能し、ユーザーによるパスワードの入力操作を受け付ける。暗号化部 78 は、文書データ生成部 76 で生成された文書データ D1 を、ユーザーによって指定されたパスワードを用いて暗号化することにより暗号データに変換する。そしてアップロード部 79 は、暗号化された文書データ D1 と、ユーザーによって指定されたパスワードとを情報共有サーバー 2 へアップロードする。尚、アップロード部 79 は、文書データ D1 をアップロードするとき、ユーザー情報 67 からログインユーザーに関する情報を抽出し、ログインユーザーに関する情報を情報共有サーバー 2 へ送信する。これにより、情報共有サーバー 2 は、文書データ D1 をアップロードしたユーザーを特定することができるようになる。

【0055】

印刷ジョブ実行部 72 は、通信インタフェース 63 を介して印刷ジョブや文書データ D1 を受信した場合に機能し、印刷ジョブや文書データ D1 に基づいてプリンタ部 65 を駆動することにより、画像処理装置 5 において印刷出力を行わせるものである。

【0056】

次に情報共有サーバー 2 について説明する。図 4 は、情報共有サーバー 2 のハードウェア構成及び機能構成の一例を示すブロック図である。図 4 に示すように、情報共有サーバー 2 は、CPU やメモリなどを備えて構成される制御部 10 と、各種情報を記憶する記憶部 11 と、情報処理装置 4 や画像処理装置 5 と通信を行うための通信インタフェース 12 とを備えており、一般的なコンピュータと同様のハードウェア構成を有している。記憶部 11 は、例えばハードディスクドライブ (HDD) などによって構成される不揮発性の記憶手段である。この記憶部 11 には、制御部 10 の CPU によって実行されるプログラム

10

20

30

40

50

13が予め記憶される。また記憶部11には、文書データD1を共有する複数のユーザーに関する情報が登録される共有情報14、複数のユーザーで共有される文書データD1、文書データD1に設定されるパスワード31などが記憶される。

【0057】

制御部10のCPUは、情報共有サーバー2が起動すると、記憶部11からプログラム13を読み出して実行する。これにより、制御部10は、共有情報登録部20、ユーザー認証部21、アップロードデータ取得部22、文書データ管理部23、パスワード管理部24、閲覧情報提供部25、文書データ提供部26及び印刷制御部27として機能する。

【0058】

共有情報登録部20は、管理者などの設定操作に基づき、情報を共有する複数のユーザーに関する情報などを共有情報14に登録する処理部である。例えば、共有情報登録部20は、情報共有サーバー2に管理者がログインした場合に機能し、管理者による設定操作に基づき、情報を共有するグループや、そのグループにおいて他のユーザーと情報を共有することが可能なユーザーに関する情報を共有情報14に登録する。

10

【0059】

図5は、共有情報14の一例を示す図である。図5に示すように、共有情報14は、グループ情報14aと、共有ユーザー情報14bと、認証情報14cと、暗号鍵14dと、復号鍵14eと、識別情報14fとを含む情報である。図5では、情報を共有するグループとして、グループXとグループYの2つのグループが登録された例を示している。グループXでは、情報を共有するユーザーとして、4人のユーザーA、B、C、Dが登録されている。そのため、グループXに属する4人のユーザーA、B、C、Dは、グループXに対してアップロードされる文書データD1を共有することができる。またグループYでは、情報を共有するユーザーとして、別の4人のユーザーE、F、G、Hが登録されている。そのため、グループYに属する4人のユーザーE、F、G、Hは、グループYに対してアップロードされる文書データD1を共有することができる。このようなグループ管理により、情報共有サーバー2は、ユーザーがログインするときに、そのログインユーザーが所属するグループを特定することができるようになり、ログインユーザーが所属するグループにアップロードされた文書データD1だけをログインユーザーに公開できると共に、ログインユーザーが所属していないグループにアップロードされた文書データD1をログインユーザーに公開しないように制限することができる。

20

30

【0060】

認証情報14cは、個々のユーザーを識別するための情報であり、例えば各ユーザーに対して個別に付与されるランダムな文字列などによって構成される。尚、認証情報14cは、ユーザーIDとパスワードとの組み合わせによって構成される情報であっても構わない。この認証情報14cは、ユーザーからのログイン要求を受け付けた場合に、そのユーザーを認証するために用いられる。

【0061】

暗号鍵14dは、例えば管理者によってグループ毎に設定される鍵情報であり、暗号化された文書データD1を復号する際に用いるパスワードを暗号化する鍵情報である。復号鍵14eは、暗号鍵14dと対をなす復号用の鍵情報であり、例えば管理者によってグループ毎に設定され、暗号化されたパスワードを復号するために用いられる。

40

【0062】

識別情報14fは、例えば管理者によってグループ毎に設定されるユニークな情報である。この識別情報14fは、例えば4～8桁程度の暗証番号(PINコード)などで構成される。

【0063】

ただし、識別情報14fは、図5に示すように復号鍵14eと別に管理されるものではなく、復号鍵14eを利用するために予め復号鍵14eに設定される情報であっても構わない。例えば、復号鍵14eを生成するときのオプション機能として、復号鍵14eに識別情報14fを設定する機能がある。そのようなオプション機能を用いて、復号鍵14e

50

に識別情報 1 4 f が設定されたものであれば、共有情報 1 4 において、復号鍵 1 4 e とは別に識別情報 1 4 f を記憶しておく必要はない。この場合、例えば復号鍵 1 4 e は、識別情報 1 4 f によって暗号化された情報となる。

【 0 0 6 4 】

共有情報登録部 2 0 は、共有情報 1 4 に対して新規グループを登録すると、その新規グループに対して登録された複数のユーザーのそれぞれに対し、認証情報 1 4 c 及び識別情報 1 4 f を個別に通知する。また共有情報登録部 2 0 は、共有情報 1 4 に登録されている既存のグループに対して新規ユーザーを登録した場合、その新規ユーザーに認証情報 1 4 c 及び識別情報 1 4 f を通知する。また共有情報登録部 2 0 は、各ユーザーに対して認証情報 1 4 c 及び識別情報 1 4 f を通知するとき、情報共有サーバー 2 へアクセスするためのアドレス情報などを添付して通知する。したがって、このような通知を受けたユーザーは、自身の情報処理装置 4 を操作することにより情報共有サーバー 2 へアクセスすることが可能になると共に、情報共有サーバー 2 へログインするための認証情報 1 4 c、及び、自身が属するグループに付与されている固有の識別情報 1 4 f を把握することができる。尚、共有情報登録部 2 0 による通知は例えば電子メールなどによって行われる。

10

【 0 0 6 5 】

ユーザー認証部 2 1 は、通信インタフェース 1 2 が情報処理装置 4 からのログイン要求を受け付けた場合に機能し、ユーザー認証処理を行う。ユーザー認証部 2 1 は、ログイン要求に含まれる情報が、共有情報 1 4 においてユーザー毎に登録されている認証情報 1 4 c に一致するか否かを判断することによりユーザー認証処理を行う。ログイン要求に含まれる情報が認証情報 1 4 c に一致する場合、認証成功となり、ユーザー認証部 2 1 は、その認証情報 1 4 c に対応するユーザーと、そのユーザーが属するグループとを特定する。そしてユーザー認証部 2 1 は、そのグループに対してアップロードされている文書データ D 1 をユーザーが利用可能なログイン状態へ移行させる。これに対し、ログイン要求に含まれる情報が認証情報 1 4 c に一致しない場合、認証失敗となるため、ユーザー認証部 2 1 は、ログイン状態へは移行させない。

20

【 0 0 6 6 】

アップロードデータ取得部 2 2 は、通信インタフェース 1 2 がアップロードデータを受信した場合に機能し、情報処理装置 4 又は画像処理装置 5 からのアップロードデータを取得する処理部である。アップロードデータ取得部 2 2 は、アップロードデータを取得すると、そのアップロードデータに含まれる情報からアップロードユーザーを特定し、共有情報 1 4 を参照することにより、そのアップロードユーザーが属するグループを特定する。

30

【 0 0 6 7 】

またアップロードデータ取得部 2 2 は、アップロードデータに暗号化された文書データ D 1 と、パスワードとが含まれる場合、アップロードデータから文書データ D 1 とパスワードとを分類する。そして暗号化された文書データ D 1 を文書データ管理部 2 3 へ出力し、パスワードをパスワード管理部 2 4 へ出力する。またアップロードデータ取得部 2 2 は、アップロードデータに含まれるパスワードを暗号化してパスワード管理部 2 4 へ出力するように構成される。

40

【 0 0 6 8 】

図 6 は、アップロードデータ取得部 2 2 による暗号化処理の概念を示す図である。図 6 に示すようにアップロードデータ取得部 2 2 は、暗号化部 2 2 a を備えている。この暗号化部 2 2 a は、情報処理装置 4 又は画像処理装置 5 から受信したアップロードデータにパスワードが含まれる場合に機能する。そして暗号化部 2 2 a は、アップロードデータを送信したユーザーが属するグループに登録されている暗号鍵 1 4 d を共有情報 1 4 から読み出し、情報処理装置 4 又は画像処理装置 5 から受信したパスワード 3 0 をその暗号鍵 1 4 d で暗号化する。すなわち、暗号化部 2 2 a は、文書データ D 1 が共有されるグループに対して予め設定されている暗号鍵 1 4 d を用いてパスワード 3 0 を暗号化することにより、暗号化パスワード 3 1 を生成するのである。そしてアップロードデータ取得部 2 2 は、その暗号化パスワード 3 1 をパスワード管理部 2 4 へ出力する。

50

【 0 0 6 9 】

文書データ管理部 2 3 は、アップロードデータ取得部 2 2 から出力される文書データ D 1 を記憶部 1 1 に保存して管理する。またパスワード管理部 2 4 は、アップロードデータ取得部 2 2 から出力される暗号化パスワード 3 1 を記憶部 1 1 に保存して管理する。これらの文書データ管理部 2 3 とパスワード管理部 2 4 は、暗号化された文書データ D 1 と、暗号化パスワード 3 1 とを相互に関連付けた管理情報 3 5 を生成し、その管理情報 3 5 を共有することで、暗号化された文書データ D 1 と暗号化パスワード 3 1 とを 1 対 1 で関連付けて管理する。

【 0 0 7 0 】

図 7 は、管理情報 3 5 の一例を示す図である。管理情報 3 5 には、グループ情報 3 5 a と、共有文書ファイル名情報 3 5 b と、アップロードユーザー情報 3 5 c と、パスワード情報 3 5 d とが含まれる。グループ情報 3 5 a は、文書データ D 1 が共有されるグループを示す情報である。共有文書ファイル名情報 3 5 b は、共有される文書データ D 1 のファイル名を示す情報である。アップロードユーザー情報 3 5 c は、文書データ D 1 をアップロードしたユーザーを示す情報である。パスワード情報 3 5 d は、文書データ D 1 を復号するパスワード 3 0 が暗号化された暗号化パスワード 3 1 を特定するための情報である。したがって、図 7 に示す管理情報 3 5 を参照すれば、記憶部 1 1 に記憶される文書データ D 1 がどのグループに共有されるデータであるかを特定できると共に、個々の文書データ D 1 に対応する暗号化パスワード 3 1 を特定することも可能である。また管理情報 3 5 を参照すれば、文書データ D 1 のアップロードユーザーも特定することができる。文書データ管理部 2 3 及びパスワード管理部 2 4 によってこのような管理情報 3 5 が共有して管理されることにより、暗号化された文書データ D 1 は、共有対象となるグループ、アップロードユーザー及び暗号化パスワード 3 1 を特定することが可能な状態で記憶部 1 1 に保存されることになる。

【 0 0 7 1 】

閲覧情報提供部 2 5 は、情報共有サーバー 2 がログインユーザーによるログイン状態へ移行することにより機能し、ログインユーザーが共有可能な文書データ D 1 の閲覧情報を提供する処理部である。例えば、閲覧情報提供部 2 5 は、ログインユーザーによるログイン状態となると、共有情報 1 4 を参照することによってそのログインユーザーが属するグループを特定する。そして閲覧情報提供部 2 5 は、文書データ管理部 2 3 に対して特定したグループを通知し、文書データ管理部 2 3 からログインユーザーが属するグループにおいて共有されている文書データ D 1 の一覧情報を取得する。閲覧情報提供部 2 5 は、その一覧情報に基づき、ログインユーザーが操作する情報処理装置 4 に対して一覧情報を提供する。これにより、ログインユーザーは、自身が閲覧可能な文書データ D 1 の一覧を把握することができ、その一覧の中から所望の文書データ D 1 を選択して情報共有サーバー 2 に閲覧要求を送信することができる。

【 0 0 7 2 】

閲覧情報提供部 2 5 は、ログインユーザーの情報処理装置 4 から文書データ D 1 を指定した閲覧要求を受信すると、復号部 2 5 a、閲覧情報生成部 2 5 b 及び閲覧情報送信部 2 5 c を順次機能させる。

【 0 0 7 3 】

復号部 2 5 a は、ログインユーザーによって指定された文書データ D 1 であって、暗号化された文書データ D 1 を復号する処理部である。図 8 は、この復号部 2 5 a の詳細な機能構成の一例を示す図である。復号部 2 5 a は、図 8 に示すように、識別情報受付部 8 1 と、識別情報判定部 8 2 と、復号鍵取得部 8 3 と、パスワード復号部 8 4 と、文書データ復号部 8 5 とを備えている。

【 0 0 7 4 】

識別情報受付部 8 1 は、ログインユーザーによる識別情報の入力操作を受け付ける処理部である。この識別情報受付部 8 1 は、ログインユーザーの情報処理装置 4 に対して識別情報の入力操作を促す識別情報入力画面を送信する。その後、識別情報受付部 8 1 は、口

10

20

30

40

50

ログインユーザーが識別情報入力画面に対して入力した識別情報を受信すると、その識別情報を識別情報判定部 8 2 へ出力する。

【 0 0 7 5 】

識別情報判定部 8 2 は、ログインユーザーによって入力された識別情報が共有情報 1 4 に登録されている識別情報 1 4 f に一致するか否かを判定する処理部である。すなわち、識別情報判定部 8 2 は、識別情報受付部 8 1 からログインユーザーによって入力された識別情報を取得すると、共有情報 1 4 を参照し、その識別情報がログインユーザーの属するグループに登録されている識別情報 1 4 f と一致するか否かを判定する。このようにユーザーが情報共有サーバー 2 にログインしている状態であっても、さらにログインユーザーに識別情報の入力を促して共有情報 1 4 に予め登録されている識別情報 1 4 f と一致するか否かを判定することにより、ログインユーザーのなりすましによって文書データ D 1 が閲覧されてしまうことを未然に防止することができ、セキュリティの高いシステムが実現される。

10

【 0 0 7 6 】

復号鍵取得部 8 3 は、識別情報判定部 8 2 によってログインユーザーの入力した識別情報が共有情報 1 4 に登録されている識別情報 1 4 f と一致した場合に機能する。そして復号鍵取得部 8 3 は、共有情報 1 4 を参照し、ログインユーザーの属するグループに登録されている復号鍵 1 4 e を取得する。復号鍵取得部 8 3 が復号鍵 1 4 e を取得すると、その復号鍵 1 4 e をパスワード復号部 8 4 へ出力する。

【 0 0 7 7 】

尚、上述したように、復号鍵 1 4 e に識別情報 1 4 f が設定されている場合には、上述した識別情報判定部 8 2 は特に必要ではない。すなわち、この場合は、復号鍵取得部 8 3 がログインユーザーによって入力された識別情報 1 4 f を用いて復号鍵 1 4 e を取得するようにすれば良い。例えばログインユーザーによって入力された識別情報 1 4 f を用いて暗号化された復号鍵 1 4 e を復号するのである。そして復号鍵取得部 8 3 は、識別情報 1 4 f を用いて取得した復号鍵 1 4 e をパスワード復号部 8 4 へ出力する。ただし、ログインユーザーによって入力された識別情報 1 4 f を用いても、ログインユーザーの属するグループに登録されている復号鍵 1 4 e を正常に取得することができないこともある。例えば、ログインユーザーによって入力された識別情報 1 4 f では、復号鍵 1 4 e を正常に復号することができない場合などである。そのような場合、これ以後の処理は行われないので、ログインユーザーのなりすましによって文書データ D 1 が不正に閲覧されてしまうことを未然に防止することができる。

20

30

【 0 0 7 8 】

パスワード復号部 8 4 は、復号鍵 1 4 e を取得すると、パスワード管理部 2 4 に対し、ログインユーザーが指定した暗号化された文書データ D 1 を復号するための暗号化パスワード 3 1 を問い合わせる。その後、パスワード復号部 8 4 は、パスワード管理部 2 4 からの回答に基づき、記憶部 1 1 から暗号化パスワード 3 1 を読み出して取得する。そしてパスワード復号部 8 4 は、復号鍵取得部 8 3 から取得した復号鍵 1 4 e を用いて暗号化パスワード 3 1 を復号する。これにより、暗号化パスワード 3 1 は、ログインユーザーが指定した暗号化された文書データ D 1 を復号する際に用いられるパスワード 3 0 に復元される。

40

【 0 0 7 9 】

続いて文書データ復号部 8 5 が機能する。文書データ復号部 8 5 は、パスワード復号部 8 4 から復号されたパスワード 3 0 を取得すると、文書データ管理部 2 3 に対し、ログインユーザーが指定した暗号化された文書データ D 1 を問い合わせる。その後、文書データ復号部 8 5 は、文書データ管理部 2 3 からの回答に基づき、記憶部 1 1 から閲覧対象として指定された暗号化された文書データ D 1 を読み出して取得する。そして文書データ復号部 8 5 は、復号されたパスワード 3 0 を用いて暗号化された文書データ D 1 を復号する。これにより、暗号化された文書データ D 1 は、その中身を閲覧することが可能な文書データ D 2 に変換される。

50

【 0 0 8 0 】

図 4 に戻り、上記のようにして復号された文書データ D 2 が生成されると、次に閲覧情報提供部 2 5 において閲覧情報生成部 2 5 b が機能する。閲覧情報生成部 2 5 b は、復号された文書データ D 2 に基づいて閲覧用画像を生成し、その閲覧用画像を含む閲覧画面を生成する処理部である。図 9 は、閲覧情報生成部 2 5 b の詳細な機能構成の一例を示す図である。閲覧情報生成部 2 5 b は、図 9 に示すように、閲覧用画像生成部 9 1 と、閲覧画面生成部 9 2 とを備えている。また閲覧画面生成部 9 2 は、保存禁止設定部 9 2 a と、印刷禁止設定部 9 2 b とを備えている。

【 0 0 8 1 】

閲覧用画像生成部 9 1 は、復号された文書データ D 2 に基づいて閲覧用画像を生成するものである。この閲覧用画像は、例えばビットマップなどの画像データであり、文書データ D 2 に含まれるテキストなどのコンテンツをそのまま画像化したプレビュー用の画像データである。そのため、ログインユーザーが情報処理装置 4 に表示される閲覧用画像を閲覧しているときに、文書データ D 2 に含まれるテキストなどのコンテンツデータがオリジナルデータのままでコピーされてしまうことを未然に防止することができる。

10

【 0 0 8 2 】

閲覧画面生成部 9 2 は、閲覧用画像生成部 9 1 によって文書データ D 2 に基づく閲覧用画像が生成されると、その閲覧用画像を含む閲覧画面を生成する。この閲覧画面は、例えば H T T P (Hypertext Transfer Protocol) など記述された W e b ページとして生成される。また閲覧情報送信部 2 5 c は、閲覧画面を生成するとき、保存禁止設定部 9 2 a

20

【 0 0 8 3 】

保存禁止設定部 9 2 a は、情報処理装置 4 において起動されている W e b ブラウザ 4 8 の閲覧画面の保存機能を無効にする処理部である。例えば保存禁止設定部 9 2 a は、W e b ページとして生成される閲覧画面に、W e b ブラウザ 4 8 の保存機能を無効にするコマンドを組み込むことにより、閲覧画面の保存禁止設定を行う。そのため、ログインユーザーが情報処理装置 4 に表示される閲覧画面を閲覧しているときに、W e b ブラウザ 4 8 の保存機能により、情報共有サーバー 2 が関与できない状態で閲覧用画像が保存されてしまうことを防止することができる。

【 0 0 8 4 】

また印刷禁止設定部 9 2 b は、情報処理装置 4 において起動されている W e b ブラウザ 4 8 の閲覧画面の印刷機能を無効にする処理部である。例えば印刷禁止設定部 9 2 b は、上記と同様、W e b ページとして生成される閲覧画面に、W e b ブラウザ 4 8 の印刷機能を無効にするコマンドを組み込むことにより、閲覧画面の印刷禁止設定を行う。そのため、ログインユーザーが情報処理装置 4 に表示される閲覧画面を閲覧しているときに、W e b ブラウザ 4 8 の印刷機能により、情報共有サーバー 2 が関与できない状態で閲覧用画像が印刷出力されてしまうことを防止することができる。

30

【 0 0 8 5 】

再び図 4 に戻り、上記のようにして閲覧画面が生成されると、次に閲覧情報提供部 2 5 において閲覧情報送信部 2 5 c が機能する。閲覧情報送信部 2 5 c は、閲覧情報生成部 2 5 b によって生成された閲覧用画像を含む閲覧画面を、閲覧要求の送信元であるログインユーザーの情報処理装置 4 へ送信する。これにより、ログインユーザーの情報処理装置 4 は、W e b ブラウザ 4 8 の機能によって情報共有サーバー 2 から取得した閲覧画面を表示部 4 2 に表示する。

40

【 0 0 8 6 】

図 1 0 は、情報処理装置 4 において表示される閲覧画面 G 1 の一例を示す図である。この閲覧画面 G 1 は、情報処理装置 4 において起動されている W e b ブラウザ 4 8 によって表示される画面である。例えば閲覧画面 G 1 の中央の表示領域 R 1 には、図 1 0 に示すように復号された文書データ D 2 に基づく閲覧用画像が表示される。ただし、この閲覧画面 G 1 には上述した保存禁止設定や印刷禁止設定が施されているため、ログインユーザーは

50

、Webブラウザ48の機能を利用した閲覧画面G1の保存や印刷を行うことはできない。

【0087】

また図10に示すように、閲覧画面G1の下部には、文書一覧ボタンB1と、ダウンロードボタンB2と、印刷ボタンB3と、終了ボタンB4とが含まれている。文書一覧ボタンB1は、ログインユーザーが閲覧可能な文書一覧を情報共有サーバ2へ要求するボタンである。ダウンロードボタンB2は、現在閲覧中である文書データD1のダウンロードを情報共有サーバ2へ要求するボタンである。印刷ボタンB3は、現在閲覧中である文書データD1の印刷を情報共有サーバ2へ要求するボタンである。さらに終了ボタンB4は、文書データD1の閲覧を終了することを情報共有サーバ2へ通知するボタンである。

10

【0088】

ログインユーザーは、現在閲覧中である文書データD1を入手したい場合、ダウンロードボタンB2を操作する。これにより、Webブラウザ48は、情報共有サーバ2へダウンロード要求を送信する。またログインユーザーは、現在閲覧中である文書データD1を印刷したい場合、印刷ボタンB3を操作する。これにより、Webブラウザ48は、情報共有サーバ2へ印刷要求を送信する。

【0089】

図4に戻り、文書データ提供部26は、情報共有サーバ2が情報処理装置4からダウンロード要求を受信した場合に機能し、ログインユーザーによって指定された文書データD1をダウンロード要求の送信元である情報処理装置4へ提供する処理部である。この文書データ提供部26は、データ送信部26aと、通知部26bとを備えている。

20

【0090】

データ送信部26aは、ダウンロード対象である暗号化された文書データD1を記憶部11から取得すると共に、その暗号化された文書データD1を復号するためのパスワード30を閲覧情報提供部25から取得する。尚、データ送信部26aは、記憶部11から暗号化パスワード31を読み出し、復号鍵14eを用いて暗号化パスワード31を復号することにより、パスワード30を取得するようにしても良い。そしてデータ送信部26aは、暗号化された文書データD1と、パスワード30とを、ダウンロード要求の送信元であるログインユーザーの情報処理装置4へ送信する。これにより、ログインユーザーは、暗号化された文書データD1及びパスワード30をダウンロード取得することができるため、パスワード30を用いて暗号化された文書データD1を復号することにより、文書データD1を利用することができるようになる。

30

【0091】

またデータ送信部26aは、暗号化された文書データD1とパスワード30とをそれぞれ異なる通信経路で送信するようにしても良い。例えば、データ送信部26aは、暗号化された文書データD1を情報処理装置4のWebブラウザ48に対して送信し、パスワード30を電子メールなどによってログインユーザーへ送信するようにしても良い。このように暗号化された文書データD1とパスワード30とをそれぞれ異なる通信経路で送信することにより、セキュリティのより一層高いシステムが実現される。

40

【0092】

通知部26bは、データ送信部26aによって暗号化された文書データD1とパスワード30の送信が行われることに伴い、文書データD1をアップロードしたユーザーに対して文書データD1がダウンロードされたことを通知する処理部である。通知部26bがアップロードユーザーに対して通知を行う際には、文書データD1をダウンロードしたユーザーや、ダウンロード日時なども通知することが好ましい。また通知部26bは、文書データD1のアップロードユーザーだけではなく、同じグループに属する全てのユーザーに通知を行うようにしても良いし、また管理者にも通知を行うようにしても良い。

【0093】

印刷制御部27は、情報共有サーバ2が情報処理装置4から印刷要求を受信した場合

50

に機能するものである。印刷制御部 27 は、ログインユーザーによって指定された文書データ D 1 を、ログインユーザーによって指定された印刷装置へ送信する。印刷制御部 27 は、印刷要求を受信すると、印刷要求の送信元である情報処理装置 4 と同じローカルネットワークに存在する印刷装置を検索する。その結果、情報処理装置 4 と同じローカルネットワーク内に印刷装置が存在する場合、印刷制御部 27 は、その印刷装置をログインユーザーに提示し、ログインユーザーによる印刷装置の指定操作を受け付ける。尚、検索によって印刷装置が見付からなかった場合、印刷制御部 27 は、ログインユーザーによる印刷装置の手動設定操作を受け付け、その手動設定操作に基づいて印刷データの送信先となる印刷装置を特定する。このような印刷制御部 27 は、印刷データ送信部 27 a と、通知部 27 b とを備えている。

10

【0094】

印刷データ送信部 27 a は、印刷データの送信先として特定された印刷装置に対して印刷データを送信する処理部である。この印刷データ送信部 27 a は、印刷データの送信先として特定された印刷装置に対応するプリンタドライバがインストールされているか否かを判断し、プリンタドライバがインストールされていれば、そのプリンタドライバを起動し、特定された印刷装置において実行可能な印刷ジョブを生成する。すなわち、印刷データ送信部 27 a は、プリンタドライバを起動して印刷ジョブを印刷装置へ送信する場合、復号された文書データ D 2 に基づいて印刷ジョブを生成し、その印刷ジョブを印刷装置へ送信する。

20

【0095】

これに対し、印刷データの送信先として特定された印刷装置に対応するプリンタドライバがインストールされていない場合、印刷データ送信部 27 a は、特定された印刷装置がダイレクトプリント対応機種であると判断し、文書データ D 1 をそのまま印刷装置へ送信する。すなわち、印刷装置がダイレクトプリント対応機種である場合、印刷データ送信部 27 a は、暗号化された文書データ D 1 と、その文書データ D 1 を復号するためのパスワード 30 とを印刷装置へ送信し、印刷装置において暗号化された文書データ D 1 を復号させることによって印刷可能な文書データ D 2 を生成させて印刷出力を行わせる。

【0096】

例えば上述した画像処理装置 5 が印刷装置として特定された場合、画像処理装置 5 は、情報共有サーバー 2 から、暗号化された文書データ D 1 とパスワード 30 とを受信する。これに伴い、画像処理装置 5 において印刷ジョブ実行部 7 2 が動作する。そして印刷ジョブ実行部 7 2 は、パスワード 30 を用いて暗号化された文書データ D 1 を復号する。これにより、印刷ジョブ実行部 7 2 は、印刷可能な文書データ D 2 を取得することができる。そして印刷ジョブ実行部 7 2 は、復号した文書データ D 2 に基づいて印刷出力を行う。したがって、この場合、情報共有サーバー 2 は、画像処理装置 5 に対応するプリンタドライバをインストールしていなくても、画像処理装置 5 に印刷出力を行わせることができるため、情報共有サーバー 2 の負荷を軽減することができる。

30

【0097】

通知部 27 b は、印刷データ送信部 27 a によって印刷データが印刷装置へ送信されることに伴い、文書データ D 1 をアップロードしたユーザーに対して印刷出力が行われたことを通知する処理部である。通知部 27 b がアップロードユーザーに対して通知を行う際には、印刷出力を行ったユーザーや、印刷日時なども通知することが好ましい。また通知部 27 b は、文書データ D 1 のアップロードユーザーだけではなく、同じグループに属する全てのユーザーに通知を行うようにしても良いし、また管理者にも通知を行うようにしても良い。

40

【0098】

このように情報共有サーバー 2 は、ログインユーザーによって文書データ D 1 のダウンロードや印刷出力が行われると、それをログインユーザーとは異なる他のユーザーであって、少なくとも同一グループに属するユーザーに通知するため、万一、文書データ D 1 が第三者に漏洩した場合には漏洩元を速やかに特定することができるという利点がある。

50

【 0 0 9 9 】

次に上記のような情報共有システム 1 において行われる動作の概要について説明する。図 1 1 は、ユーザー A が文書データ D 1 を情報共有サーバー 2 へアップロードし、ユーザー B がその文書データ D 1 を閲覧する場合の動作シーケンスを示す図である。尚、図 1 1 では、ユーザー A が情報処理装置 4 a を操作し、ユーザー B が情報処理装置 4 b を操作する場合を例示している。

【 0 1 0 0 】

まずユーザー A は、情報処理装置 4 a を操作することにより、情報共有サーバー 2 へのアップロード対象となる文書データ D 1 を作成する（プロセス P 1 0）。その文書データ D 1 が機密情報を含んでいる場合、ユーザー A は、情報処理装置 4 a に対してパスワード 3 0 を入力し（プロセス P 1 1）、文書データ D 1 をそのパスワード 3 0 で暗号化する（プロセス P 1 2）。その後、ユーザー A は、情報処理装置 4 a を操作することによって情報共有サーバー 2 へログインし、情報共有サーバー 2 へ暗号化された文書データ D 1 をアップロードする。このとき、情報処理装置 4 a は、暗号化された文書データ D 1 を復号するためのパスワード 3 0 を情報共有サーバー 2 へ送信する。

10

【 0 1 0 1 】

情報共有サーバー 2 は、情報処理装置 4 a から暗号化された文書データ D 1 とパスワード 3 0 とを受信すると、共有情報 1 4 を参照することにより、ユーザー A が属するグループを特定し、ユーザー A が属するグループに設定されている暗号鍵 1 4 d を取得する。そして情報共有サーバー 2 は、情報処理装置 4 a から受信したパスワード 3 0 を暗号鍵 1 4 d で暗号化し、暗号化パスワード 3 1 を生成する（プロセス P 1 3）。続いて情報共有サーバー 2 は、暗号化された文書データ D 1 と、暗号化パスワード 3 1 とを相互に関連付けて記憶部 1 1 へ保存する（プロセス P 1 4）。このとき、情報処理装置 4 a から受信したパスワード 3 0 は、暗号化された暗号化パスワード 3 1 として記憶部 1 1 に保存されるため、仮に暗号化された文書データ D 1 と暗号化パスワード 3 1 とが不正に読み出されたとしても、暗号化された文書データ D 1 を復号することはできず、情報漏洩を防止することができる。尚、情報共有サーバー 2 は、情報処理装置 4 a から受信したパスワード 3 0 を暗号鍵 1 4 d で暗号化することに伴い、オリジナルのパスワード 3 0 を削除しておくことが好ましい。そして情報共有サーバー 2 は、ユーザー A によってアップロードされた文書データ D 1 を、ユーザー A と同じグループに属する他のユーザーに公開する。

20

30

【 0 1 0 2 】

ユーザー A と同一グループに属するユーザー B は、文書データ D 1 を閲覧するとき、情報処理装置 4 b を操作することによって Web ブラウザ 4 8 を起動し、情報共有サーバー 2 にアクセスする。これにより、情報処理装置 4 b には情報共有サーバー 2 にログインするための画面が表示される。ユーザー B は、その画面に対して事前に通知されている自身の認証情報 1 4 c を入力し、情報共有サーバー 2 に対してログイン要求 D 1 0 を送信する。情報共有サーバー 2 は、ログイン要求 D 1 0 を受信すると、ユーザー認証を行い（プロセス P 1 5）、ユーザー B が共有情報 1 4 に登録された正規ユーザーであれば、ユーザー B が閲覧可能な文書データ D 1 の一覧を情報処理装置 4 b へ送信する。これにより、ユーザー B は、自身が所属するグループにおいて公開されている文書データ D 1 の一覧を入手することができ、その一覧の中から一の文書データ D 1 を指定した閲覧要求 D 1 1 を情報共有サーバー 2 へ送信することができるようになる。

40

【 0 1 0 3 】

情報共有サーバー 2 は、情報処理装置 4 b から閲覧要求 D 1 1 を受信すると、ユーザー B が所属するグループに登録されている復号鍵 1 4 e を読み出し、閲覧対象として指定された文書データ D 1 に関連付けられている暗号化パスワード 3 1 を復号する（プロセス P 1 6）。これにより、暗号化パスワード 3 1 は、暗号化された文書データ D 1 を復号するためのパスワード 3 0 に変換される。そして情報共有サーバー 2 は、その復号されたパスワード 3 0 を用いて、暗号化された文書データ D 1 を復号する（プロセス P 1 7）。これにより、暗号化された文書データ D 1 は、閲覧可能な文書データ D 2 に復号される。その

50

後、情報共有サーバー 2 は、復号された文書データ D 2 に基づく閲覧用画像を含む閲覧画面 G 1 を生成し（プロセス P 1 8）、その閲覧画面 G 1 を情報処理装置 4 b へ送信する。情報処理装置 4 b は、情報共有サーバー 2 から閲覧画面 G 1 を受信すると、その閲覧画面 G 1 を表示部 4 2 に表示する。これにより、ユーザー B は、文書データ D 1 の中身を閲覧することができるようになる。したがって、ユーザー B は、ユーザー A によって文書データ D 1 に設定されたパスワードを知らなくても、文書データ D 1 の中身を閲覧することができるのである。

【0104】

次に図 1 2 は、ユーザー B が文書データ D 1 をダウンロードする場合の動作シーケンスを示す図である。ユーザー B が文書データ D 1 を閲覧しているときにダウンロードボタン B 2 を操作すると、情報処理装置 4 b は、情報共有サーバー 2 に対し、現在閲覧中の文書データ D 1 のダウンロード要求 D 1 2 を送信する。情報共有サーバー 2 は、情報処理装置 4 b からダウンロード要求 D 1 2 を受信すると、ダウンロード対象として指定された文書データ D 1 であって暗号化された文書データ D 1 を記憶部 1 1 から読み出す（プロセス P 2 0）。そして情報共有サーバー 2 は、ダウンロード対象の文書データ D 1 に関連付けている暗号化パスワード 3 1 を読み出し、復号鍵 1 4 e を用いてその暗号化パスワード 3 1 を復号する（プロセス P 2 1）。これにより、暗号化パスワード 3 1 は、暗号化された文書データ D 1 を復号するためのパスワード 3 0 に変換される。そして情報共有サーバー 2 は、暗号化された文書データ D 1 と、復号されたパスワード 3 0 とを情報処理装置 4 b へ送信する。その結果、ユーザーは、情報処理装置 4 b において暗号化された文書データ D 1 を、パスワード 3 0 を用いて復号することができるようになる。そして情報共有サーバー 2 は、文書データ D 1 のアップロードユーザーであるユーザー A に対して通知 D 1 3 を送信し、文書データ D 1 がユーザー B によってダウンロードされたことを通知する。これにより、ユーザー A は、自身が作成した機密性のある文書がユーザー B によって入手されたことをリアルタイムで把握することができる。

【0105】

次に図 1 3 は、ユーザー B が文書データ D 1 を印刷する場合の動作シーケンスを示す図である。尚、図 1 3 では、ユーザー B が画像処理装置 5 を印刷装置として指定した場合を例示している。ユーザー B が文書データ D 1 を閲覧しているときに印刷ボタン B 3 を操作すると、情報処理装置 4 b は、情報共有サーバー 2 に対し、現在閲覧中の文書データ D 1 の印刷要求 D 1 4 を送信する。情報共有サーバー 2 は、情報処理装置 4 b から印刷要求 D 1 4 を受信すると、画像処理装置 5 が印刷装置として指定されたことを検知する。そして画像処理装置 5 に対応するプリンタドライバがインストールされていない場合、情報共有サーバー 2 は、画像処理装置 5 に対して暗号化された文書データ D 1 とパスワード 3 0 とを送信することを決定する。この場合、情報共有サーバー 2 は、印刷対象として指定された文書データ D 1 であって暗号化された文書データ D 1 を記憶部 1 1 から読み出す（プロセス P 2 5）。また情報共有サーバー 2 は、印刷対象の文書データ D 1 に関連付けている暗号化パスワード 3 1 を読み出し、復号鍵 1 4 e を用いてその暗号化パスワード 3 1 を復号する（プロセス P 2 6）。これにより、暗号化パスワード 3 1 は、暗号化された文書データ D 1 を復号するためのパスワード 3 0 に変換される。そして情報共有サーバー 2 は、暗号化された文書データ D 1 と、復号されたパスワード 3 0 とを画像処理装置 5 へ送信する。

【0106】

画像処理装置 5 は、情報共有サーバー 2 から暗号化された文書データ D 1 とパスワード 3 0 とを受信すると、パスワード 3 0 を用いて暗号化された文書データ D 1 を復号する（プロセス P 2 7）。これにより、暗号化された文書データ D 1 は、印刷可能な文書データ D 2 に変換される。そして画像処理装置 5 は、復号した文書データ D 2 に基づき印刷出力を行う（プロセス P 2 8）。一方、情報共有サーバー 2 は、暗号化された文書データ D 1 とパスワード 3 0 とを画像処理装置 5 へ送信することに伴い、文書データ D 1 のアップロードユーザーであるユーザー A に対する通知処理を行う（プロセス P 2 9）。これにより

10

20

30

40

50

、ユーザー A は、自身が作成した機密性のある文書がユーザー B によって印刷出力されたことをリアルタイムで把握することができる。

【0107】

次に情報共有サーバー 2 によって行われる具体的な処理手順の一例について説明する。図 1 4 乃至図 1 8 は、情報共有サーバー 2 によって行われる処理手順の一例を示すフローチャートである。この処理は、情報共有サーバー 2 の制御部 1 0 に設けられた CPU がプログラム 1 3 を読み出して実行することにより行われる処理である。

【0108】

情報共有サーバー 2 は、この処理を開始すると、図 1 4 に示すようにまず登録処理を行うか否かを判断する（ステップ S 1）。ここでは、例えば管理者によって新規グループや新規ユーザーの登録が指示されたか否かが判断される。そして登録処理を行う場合（ステップ S 1 で YES）、情報共有サーバー 2 は、共有情報登録処理を実行する（ステップ S 2）。この共有情報登録処理（ステップ S 2）は、管理者による新規グループや新規ユーザーの登録操作に基づいて共有情報 1 4 に新規な情報を登録処理である。尚、登録処理を行わない場合は（ステップ S 1 で NO）、ステップ S 2 の処理はスキップする。

10

【0109】

続いて情報共有サーバー 2 は、情報処理装置 4 からのログイン要求 D 1 0 を受信したか否かを判断する（ステップ S 3）。ログイン要求 D 1 0 を受信した場合（ステップ S 3 で YES）、情報共有サーバー 2 は、ユーザー認証を行い（ステップ S 4）、認証成功となったか否かを判断する（ステップ S 5）。認証成功である場合（ステップ S 5 で YES）、情報共有サーバー 2 は、ログイン要求 D 1 0 を送信したユーザーをログインユーザーとしてログイン状態へ移行させる（ステップ S 6）。これにより、ログインユーザーは、自身が所属するグループで共有される文書データ D 1 の閲覧などが可能となる。ログイン状態へ移行させると、情報共有サーバー 2 は、ログインユーザーからアップロードデータを受信したか否かを判断し（ステップ S 7）、アップロードデータを受信していれば（ステップ S 7 で YES）、文書データ登録処理を実行する（ステップ S 8）。尚、この文書データ登録処理の詳細は後述する。また情報共有サーバー 2 は、ログインユーザーから閲覧要求 D 1 1 を受信したか否かを判断し（ステップ S 9）、閲覧要求 D 1 1 を受信していれば（ステップ S 9 で YES）、閲覧情報提供処理を実行する（ステップ S 1 0）。尚、この閲覧情報提供処理の詳細は後述する。続いて情報共有サーバー 2 は、ログインユーザーからダウンロード要求 D 1 2 を受信したか否かを判断し（ステップ S 1 1）、ダウンロード要求 D 1 2 を受信していれば（ステップ S 1 1 で YES）、文書データ提供処理を実行する（ステップ S 1 2）。尚、この文書データ提供処理の詳細についても後述する。さらに情報共有サーバー 2 は、ログインユーザーから印刷要求 D 1 4 を受信したか否かを判断し（ステップ S 1 3）、印刷要求 D 1 4 を受信していれば（ステップ S 1 3 で YES）、印刷制御処理を実行する（ステップ S 1 4）。尚、この印刷制御処理の詳細についても後述する。ユーザーが情報共有サーバー 2 にログインしている状態のときには（ステップ S 1 5 で NO）、上記ステップ S 7 ~ S 1 4 の処理が繰り返し行われる。これに対し、ユーザーがログインしなかった場合には（ステップ S 3 で NO 又はステップ S 5 で NO）、ステップ S 7 ~ S 1 4 の処理は行われずにスキップする。そして情報共有サーバー 2 は、上記ステップ S 1 ~ S 1 5 の処理を繰り返し実行する。

20

30

40

【0110】

図 1 5 は、文書データ登録処理（ステップ S 8）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバー 2 は、この処理を開始すると、アップロードデータとして取得した文書データ D 1 を解析し（ステップ S 2 0）、文書データ D 1 が暗号化されているか否かを判断する（ステップ S 2 1）。その結果、文書データ D 1 が暗号化されている場合（ステップ S 2 1 で YES）、情報共有サーバー 2 は、暗号化された文書データ D 1 と共に、パスワード 3 0 を受信したか否かを判断する（ステップ S 2 2）。ここでパスワード 3 0 を受信していないことが判明した場合（ステップ S 2 2 で NO）、情報共有サーバー 2 は、アップロードを行った情報処理装置 4 においてパスワード要求画面を表示

50

させる（ステップS 2 3）。これにより、アップロードユーザーは、暗号化された文書データD 1を復号するためのパスワードを入力することが可能となり、情報共有サーバー2にパスワード3 0が送信される。その結果、情報共有サーバー2は、情報処理装置4からパスワード3 0を受信する（ステップS 2 4）。尚、受信したアップロードデータにパスワード3 0が含まれていれば（ステップS 2 2でYES）、ステップS 2 3, S 2 4の処理は不要である。

【0 1 1 1】

続いて情報共有サーバー2は、アップロードユーザーが属するグループを特定し、そのグループに登録されている暗号鍵1 4 dを読み出し（ステップS 2 5）、情報処理装置4から受信したパスワード3 0を暗号鍵1 4 dで暗号化する（ステップS 2 6）。これに伴い、情報共有サーバー2は、情報処理装置4から受信したパスワード3 0を破棄するようにしても良い。そして情報共有サーバー2は、暗号化された文書データD 1と、暗号化パスワード3 1とを相互に関連付けて記憶部1 1に保存する（ステップS 2 7）。

10

【0 1 1 2】

一方、アップロードデータに含まれる文書データD 1が暗号化されていない場合（ステップS 2 1でNO）、情報共有サーバー2は、文書データD 1の機密性が低いと判断し、受信した文書データD 1をそのまま記憶部1 1に保存して管理する（ステップS 2 8）。

【0 1 1 3】

次に図1 6は、閲覧情報提供処理（ステップS 1 0）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバー2は、この処理を開始すると、まず閲覧対象の文書データD 1を特定し（ステップS 3 0）。その文書データD 1が暗号化されているか否かを判断する（ステップS 3 1）。その結果、閲覧対象が暗号化された文書データD 1である場合（ステップS 3 1でYES）、情報共有サーバー2は、その暗号化された文書データD 1に関連付けられている暗号化パスワード3 1を読み出し（ステップS 3 2）、その暗号化パスワード3 1を復号するための復号鍵1 4 eを取得して（ステップS 3 3）、暗号化パスワード3 1を復号する（ステップS 3 4）。これにより、暗号化パスワード3 1は、暗号化された文書データD 1を復号可能なパスワード3 0に変換される。そして情報共有サーバー2は、復号したパスワード3 0を用いて、暗号化された文書データD 1を復号する（ステップS 3 5）。

20

【0 1 1 4】

その後、情報共有サーバー2は、復号した文書データD 2に基づいて閲覧用画像を生成すると共に（ステップS 3 6）、その閲覧用画像を含む閲覧画面G 1を生成する（ステップS 3 7）。また情報共有サーバー2は、閲覧画面G 1に対する保存禁止設定を付与すると共に（ステップS 3 8）、閲覧画面G 1に対する印刷禁止設定を付与する（ステップS 3 9）。これにより、情報処理装置4のWebブラウザ4 8の機能によって閲覧画面G 1が保存されたり、印刷出力されることを防止することができる。

30

【0 1 1 5】

これに対し、閲覧対象の文書データD 1が暗号化されていない場合（ステップS 3 1でNO）、情報共有サーバー2は、その文書データD 1に基づいて閲覧用画像を生成すると共に（ステップS 4 1）、その閲覧用画像を含む閲覧画面G 1を生成する（ステップS 4 2）。ただし、文書データD 1が暗号化されていないときには、文書データD 1に機密情報が含まれないと判断することができるため、情報処理装置4のWebブラウザ4 8による閲覧画面G 1の保存機能や印刷機能を制限する必要はない。そのため、文書データD 1が暗号化されていない場合、情報共有サーバー2は、閲覧画面G 1に対する保存禁止設定や印刷禁止設定を付与しない。

40

【0 1 1 6】

その後、情報共有サーバー2は、上記のようにして生成された閲覧画面G 1を、閲覧要求D 1 1の送信元である情報処理装置4へ送信する（ステップS 4 0）。これにより、ログインユーザーは、自身の情報処理装置4において文書データD 1の中身を閲覧することができるようになる。

50

【0117】

次に図17は、文書データ提供処理（ステップS12）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバ2は、この処理を開始すると、まずダウンロード対象の文書データD1を特定し（ステップS50）。その文書データD1が暗号化されているか否かを判断する（ステップS51）。その結果、ダウンロード対象が暗号化された文書データD1である場合（ステップS51でYES）、情報共有サーバ2は、その暗号化された文書データD1に関連付けられている暗号化パスワード31を読み出し（ステップS52）、その暗号化パスワード31を復号するための復号鍵14eを取得して（ステップS53）、暗号化パスワード31を復号する（ステップS54）。これにより、暗号化パスワード31は、暗号化された文書データD1を復号可能なパスワード30に変換される。そして情報共有サーバ2は、ダウンロード対象である暗号化された文書データD1を読み出し（ステップS55）、その暗号化された文書データD1を、ダウンロード要求D12の送信元である情報処理装置4へ送信すると共に（ステップS56）、復号されたパスワード30を情報処理装置4へ送信する（ステップS57）。その後、情報共有サーバ2は、アップロードユーザーに対して文書データD1がダウンロードされたことを通知する通知処理を行う（ステップS58）。

10

【0118】

これに対し、ダウンロード対象の文書データD1が暗号化されていない場合（ステップS51でNO）、情報共有サーバ2は、ダウンロード対象の文書データD1を読み出し（ステップS41）、その文書データD1をそのまま情報処理装置4へ送信する（ステップS42）。その後、情報共有サーバ2は、アップロードユーザーに対して文書データD1がダウンロードされたことを通知する通知処理を行う（ステップS58）。

20

【0119】

次に図18は、印刷制御処理（ステップS14）の詳細な処理手順の一例を示すフローチャートである。情報共有サーバ2は、この処理を開始すると、まず印刷対象の文書データD1を特定し（ステップS70）。その文書データD1が暗号化されているか否かを判断する（ステップS71）。その結果、印刷対象が暗号化された文書データD1である場合（ステップS71でYES）、情報共有サーバ2は、その暗号化された文書データD1に関連付けられている暗号化パスワード31を読み出し（ステップS72）、その暗号化パスワード31を復号するための復号鍵14eを取得して（ステップS73）、暗号化パスワード31を復号する（ステップS74）。これにより、暗号化パスワード31は、暗号化された文書データD1を復号可能なパスワード30に変換される。そして情報共有サーバ2は、印刷対象である暗号化された文書データD1を読み出す（ステップS75）。

30

【0120】

続いて情報共有サーバ2は、印刷装置を特定し（ステップS76）、その特定した印刷装置に対応するプリンタドライバがインストールされているか否かを判断する（ステップS77）。印刷装置に対応するプリンタドライバがインストールされている場合（ステップS77でYES）、情報共有サーバ2は、復号されたパスワード30を用いて暗号化された文書データD1を復号する（ステップS78）。そして情報共有サーバ2は、文書データD1を復号して生成された文書データD2に基づいて印刷装置で実行可能な印刷ジョブを生成し（ステップS79）、その印刷ジョブを印刷装置へ送信する（ステップS80）。

40

【0121】

これに対し、印刷装置に対応するプリンタドライバがインストールされていない場合（ステップS77でNO）、情報共有サーバ2は、暗号化された文書データD1を印刷装置へ送信すると共に（ステップS81）、復号されたパスワード30も印刷装置へ送信する（ステップS82）。これにより、印刷装置において、暗号化された文書データD1を復号して印刷出力を行うことができるようになる。

【0122】

50

また印刷対象の文書データD1が暗号されていない場合（ステップS71でNO）、情報共有サーバ2は、印刷対象である文書データD1を読み出す（ステップS84）。続いて情報共有サーバ2は、印刷装置を特定し（ステップS85）、その特定した印刷装置に対応するプリンタドライバがインストールされているか否かを判断する（ステップS86）。印刷装置に対応するプリンタドライバがインストールされている場合（ステップS86でYES）、情報共有サーバ2は、文書データD1に基づいて印刷装置で実行可能な印刷ジョブを生成し（ステップS87）、その印刷ジョブを印刷装置へ送信する（ステップS88）。また印刷装置に対応するプリンタドライバがインストールされていない場合（ステップS86でNO）、情報共有サーバ2は、文書データD1をそのまま印刷装置へ送信する（ステップS89）。これにより、印刷装置において、文書データD1に基づく印刷出力を行うことができるようになる。

10

【0123】

その後、情報共有サーバ2は、アップロードユーザーに対して文書データD1が印刷出力されたことを通知する通知処理を行う（ステップS90）。したがって、アップロードユーザーは、自身がアップロードした文書データD1がどのユーザーによって印刷出力されたかを把握することができる。

【0124】

以上のように、本実施形態の情報共有システム1は、情報共有サーバ2が情報処理装置4において暗号化された文書データD1を取得すると、その暗号化された文書データD1を復号するためのパスワード30を取得することができ、暗号化された文書データD1とパスワード30とを相互に関連付けて記憶する。そして暗号化された文書データD1の閲覧権限を有する他のユーザーから暗号化された文書データD1の閲覧要求D11などを取得すると、情報共有サーバ2は、暗号化された文書データD1に関連付けて管理しているパスワード30を用いて暗号化された文書データD1を復号し、他のユーザーが閲覧可能な態様で文書データD1に基づく閲覧情報を提供する。そのため、他のユーザーは、暗号化された文書データD1に設定されているパスワードを知らなくてもその文書データD1の中身を閲覧することが可能であり、特に機密文書を複数のユーザー間で共有して利用する際の利便性が向上する。

20

【0125】

また本実施形態の情報共有サーバ2は、閲覧権限を有するユーザーに対して暗号化された文書データD1の閲覧情報を提供する際、復号した文書データD2をそのまま提供するのではなく、復号した文書データD2に基づく閲覧用画像を生成し、その閲覧用画像を含む閲覧画面を提供するように構成される。そのため、復号された文書データD2に含まれるテキストなどのコンテンツデータがオリジナルデータのままでコピーされてしまうことを防止できるので、情報漏洩し難い態様で閲覧情報が提供されているのである。

30

【0126】

また本実施形態では、情報共有サーバ2が暗号化された文書データD1を復号するためのパスワード30をそのまま保存して管理するのではなく、グループ毎に設定される暗号鍵14dを用いてパスワード30を暗号化することにより、暗号化パスワード31に変換した状態で管理する構成である。そのため、仮に、暗号化された文書データD1と、それに関連付けられた暗号化パスワード31とが外部に流出したとしても、それだけでは暗号化された文書データD1を復号することができないため、セキュリティの高い情報管理が実現されている。

40

【0127】

（第2実施形態）

次に本発明の第2実施形態について説明する。上述した第1実施形態では、暗号化された文書データD1を復号するパスワード30を、情報共有サーバ2において暗号化する場合を例示した。これに対し、本実施形態では、情報処理装置4又は画像処理装置5が情報共有サーバ2に対して暗号化された文書データD1をアップロードする際に、情報処理装置4又は画像処理装置5において暗号化された文書データD1を復号するパスワード

50

30を暗号化する形態について説明する。

【0128】

図19は、本実施形態においてユーザーAが情報処理装置4aを操作することにより文書データD1を情報共有サーバー2へアップロードする場合の動作シーケンスを示す図である。ユーザーAは、情報処理装置4aを操作することにより、情報共有サーバー2へのアップロード対象となる文書データD1を作成する(プロセスP30)。その文書データD1が機密情報を含んでいる場合、ユーザーAは、情報処理装置4aに対してパスワード30を入力し(プロセスP31)、文書データD1をそのパスワード30で暗号化する(プロセスP32)。その後、ユーザーAは、情報処理装置4aを操作することによって情報共有サーバー2へログインし、情報共有サーバー2へ暗号化された文書データD1をアップロードする。

10

【0129】

情報共有サーバー2は、情報処理装置4aから文書データD1を受信すると、その文書データD1が暗号化されたデータであるか否かを判断し、暗号化されたデータであれば、ユーザーAの属するグループに設定されている暗号鍵14dを読み出し、その暗号鍵14dを情報処理装置4aへ送信する。これにより、情報処理装置4aは、情報共有サーバー2からユーザーAが所属するグループに対して予め設定されている暗号鍵14dを取得することができる。

【0130】

情報処理装置4aは、情報共有サーバー2から暗号鍵14dを取得すると、その暗号鍵14dを用いて、ユーザーAが文書データD1に設定したパスワード30を暗号化する(プロセスP33)。具体的には、図2に示したWebブラウザ48のアップロード部56が、ユーザーAによって入力されるパスワード30を、情報共有サーバー2から受信した暗号鍵14dを用いて暗号化する。これにより、ユーザーAが入力するパスワード30は、情報処理装置4aから情報共有サーバー2に送信されるときに情報処理装置4aにおいて暗号化パスワード31に変換される。そして情報処理装置4aは、暗号化パスワード31を情報共有サーバー2へ送信する。これにより、情報共有サーバー2は、情報処理装置4aにおいて暗号化された暗号化パスワード31を受信することができる。その後、情報共有サーバー2は、情報処理装置4aから受信した暗号化された文書データD1と、暗号化パスワード31とを相互に関連付けて保存する(プロセスP34)。

20

30

【0131】

このように情報処理装置4aにおいてパスワード30を暗号化して暗号化パスワード31を生成することにより、情報共有サーバー2においてパスワード30を暗号化する必要がなくなるため、情報共有サーバー2の処理負担を軽減することができるようになる。

【0132】

また画像処理装置5が情報共有サーバー2に対して暗号化された文書データD1を直接アップロードする場合も同様である。すなわち、図3に示したスキャンアプリケーション71のアップロード部79は、ユーザーAによって入力されるパスワード30を、情報共有サーバー2から受信した暗号鍵14dを用いて暗号化するのである。これにより、ユーザーAが入力するパスワード30は、画像処理装置5から情報共有サーバー2に送信されるときに画像処理装置5において暗号化パスワード31に変換される。そのため、情報共有サーバー2は、画像処理装置5から暗号化された文書データD1を受信した場合にその画像処理装置5に対して暗号鍵14dを送信することにより、画像処理装置5において暗号化された暗号化パスワード31を受信することができる。この場合においても、情報共有サーバー2においてパスワード30を暗号化する必要がなくなるため、情報共有サーバー2の処理負担を軽減することが可能である。

40

【0133】

また本実施形態では、パスワード30を暗号化する暗号鍵14dは情報共有サーバー2から情報処理装置4aなどの外部に流出することになるが、暗号化パスワード31を復号するための復号鍵14eを外部に流出させないため、セキュリティを低下させるものでは

50

ない。

【0134】

尚、本実施形態におけるその他の点は、第1実施形態で説明したものと同様である。

【0135】

(第3実施形態)

次に本発明の第3実施形態について説明する。例えば情報共有サーバ2に暗号化された文書データD1をアップロードするユーザーAが複数のグループに所属している場合、ユーザーAは、それら複数のグループにおいて同じ文書データD1を共有したいことがある。そのような場合において、ユーザーAは、一つのグループに対して暗号化された文書データD1をアップロードする操作を行った後、他のグループに対しても同様の操作を行わなければならないこととすると操作が煩雑になる。また情報共有サーバ2においては、同じ文書データD1であるにもかかわらず、グループが異なれば別の文書データとして管理しなければならないこととすると、重複した文書データD1が記憶部11の記憶領域を圧迫してしまうという問題もある。そこで本実施形態では、暗号化された文書データD1をアップロードするユーザーAが複数のグループで共有する文書データD1をアップロードする際の操作性を改善すると共に、情報共有サーバ2において重複した文書データD1が記憶部11の記憶領域を圧迫してしまうことがない形態について説明する。

10

【0136】

本実施形態では、例えばユーザーAが暗号化された文書データD1を情報共有サーバ2へアップロードするとき、情報共有サーバ2に対して文書データD1を共有するグループを指定する。このとき、ユーザーAは、自身が所属する複数のグループを指定することもできる。そしてユーザーAは、自身の情報処理装置4aを操作することにより、パスワード30で暗号化された文書データD1を情報共有サーバ2へアップロードする。このとき、情報処理装置4aは、暗号化された文書データD1と共に、暗号化された文書データD1を復号するためのパスワード30を情報共有サーバ2へ送信する。

20

【0137】

図4に示した情報共有サーバ2のアップロードデータ取得部22は、ユーザーAの情報処理装置4aからアップロードデータを受信すると、そのアップロードデータから暗号化された文書データD1を抽出し、その文書データD1を文書データ管理部23へ出力する。文書データ管理部23は、その暗号化された文書データD1を記憶部11に保存して管理する。

30

【0138】

またアップロードデータ取得部22は、ユーザーAによって暗号化された文書データD1を複数のグループで共有することが指定されている場合、ユーザーAによって指定された複数のグループのそれぞれに登録されている暗号鍵14dを取得する。そしてユーザーAの情報処理装置4aから受信したパスワード30を、複数のグループのそれぞれに登録されている暗号鍵14dを用いて1つずつ暗号化していき、複数のグループのそれぞれに対応する複数の暗号化パスワード31を生成する。そしてアップロードデータ取得部22は、グループ毎に生成される複数の暗号化パスワード31をパスワード管理部24へ出力する。パスワード管理部24は、それら複数の暗号化パスワード31を記憶部11へ保存し、それら複数の暗号化パスワード31を文書データ管理部23によって管理される1つの暗号化された文書データD1に関連付けて管理する。

40

【0139】

例えばユーザーAがグループXとグループXとの2つのグループに属しており、それら2つのグループX、Zを文書データD1の共有グループとして指定した場合、アップロードデータ取得部22は、グループXに登録されている暗号鍵14dを用いてパスワード30を暗号化することにより第1の暗号化パスワード31を生成すると共に、グループZに登録されている暗号鍵14dを用いてパスワード30を暗号化することにより第2の暗号化パスワード31を生成する。そして、これら2つの暗号化パスワード31は、1つの暗号化された文書データD1と関連付けて管理される。そのため、グループXに属する他の

50

ユーザーが文書データD1の閲覧要求D11を送信してきた場合、閲覧情報提供部25は、第1の暗号化パスワード31を復号して暗号化された文書データD1を復号するためのパスワード30を取得することができる。またグループZに属する他のユーザーが文書データD1の閲覧要求D11を送信してきた場合、閲覧情報提供部25は、第2の暗号化パスワード31を復号して暗号化された文書データD1を復号するためのパスワード30を取得することができる。

【0140】

したがって、本実施形態では、ユーザーAが文書データD1をアップロードする際に複数のグループで共有することを指定すれば良いため、同じアップロード操作を繰り返す必要がなく、操作性に優れている。また本実施形態では、1つの暗号化された文書データD1が、複数のグループで共有して利用されるため、重複した文書データD1が記憶部11の記憶領域を圧迫してしまうという問題も解決することができるようになる。

10

【0141】

尚、上記においては、情報共有サーバー2のアップロードデータ取得部22が、情報処理装置4aから受信したパスワード30をグループ毎に暗号鍵14dで暗号化する場合を説明した。しかし、これに限られるものではなく、例えば第2実施形態のように、アップロードデータ取得部22が、複数のグループのそれぞれに登録されている暗号鍵14dを情報処理装置4aへ送信し、情報処理装置4aにおいて暗号化された複数の暗号化パスワード31を取得するように構成しても良い。また本実施形態におけるその他の点は、第1実施形態又は第2実施形態で説明したものと同様である。

20

【0142】

(変形例)

以上、本発明に関する実施形態について説明したが、本発明は、上記実施形態において説明した内容のものに限られるものではなく、種々の変形例が適用可能である。

【0143】

例えば上記実施形態では、情報共有サーバー2がインターネットに接続されたクラウド3上に設けられる場合を例示したが、これに限られるものではない。すなわち、情報共有サーバー2は、ローカルネットワークに設けられるものであっても構わない。

【0144】

また上記実施形態では、パスワード30を暗号化するための暗号鍵14dと、復号するための復号鍵14eとが互いに対となる別の鍵情報である場合を例示した。しかし、上述した第1実施形態においては、暗号鍵14dと復号鍵14eとが別の鍵情報である必要はなく、例えばパスワードなどのような同一の鍵情報であっても構わない。

30

【符号の説明】

【0145】

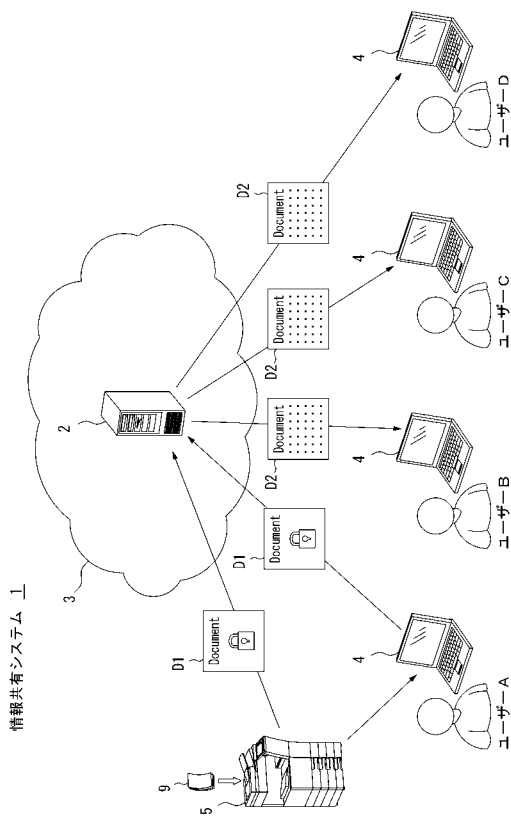
- 1 情報共有システム
- 2 情報共有サーバー
- 4 情報処理装置
- 5 画像処理装置
- 11 記憶部(記憶手段)
- 20 共有情報登録部(登録手段)
- 22 アップロードデータ取得部(取得手段)
- 25 閲覧情報提供部(閲覧情報提供手段)
- 25a 復号部(復号手段)
- 26 文書データ提供部(文書データ送信手段)
- 26b 通知部(通知手段)
- 27 印刷制御部(印刷制御手段)
- 52 文書データ暗号化部(暗号化手段)
- 56 アップロード部(アップロード手段)
- 78 暗号化部(暗号化手段)

40

50

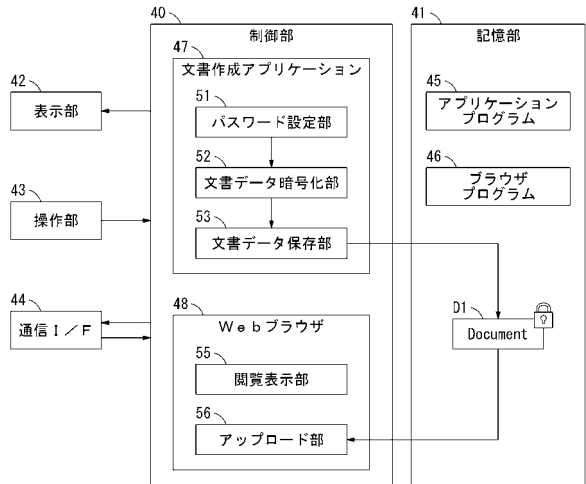
7 9 アップロード部 (アップロード手段)

【図 1】

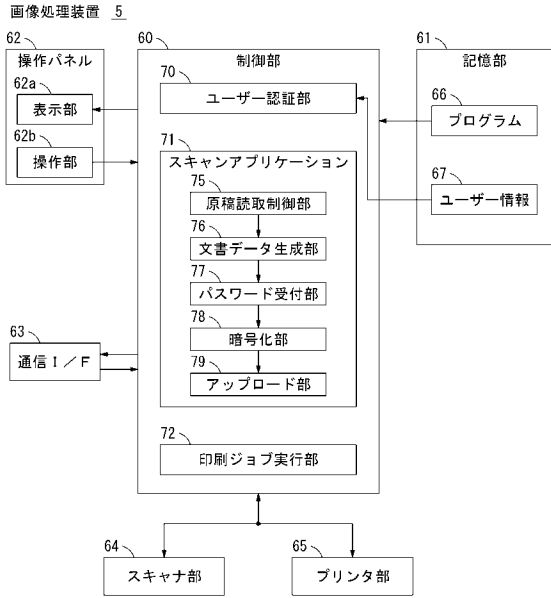


【図 2】

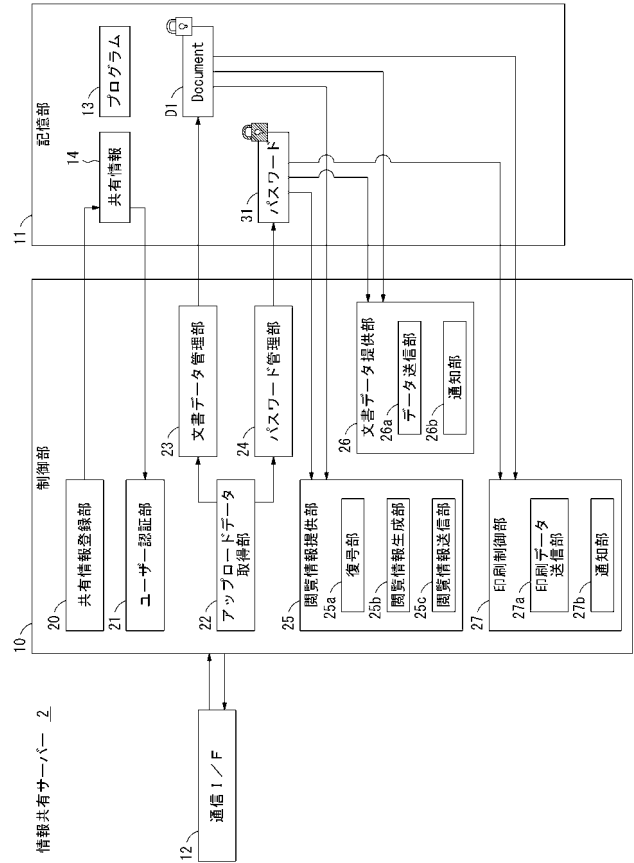
情報処理装置 4



【図3】



【図4】



【図5】

共有情報 14

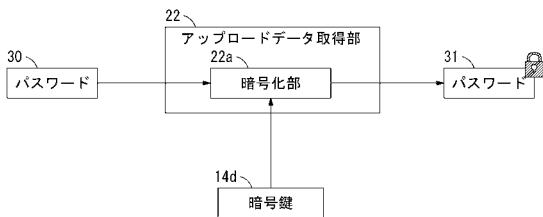
14a	14b	14c	14d	14e	14f
グループ	共有ユーザー	認証情報	暗号鍵	復号鍵	識別情報
グループX	ユーザーA	*****	key01a	key01b	6219
	ユーザーB	*****			
	ユーザーC	*****			
	ユーザーD	*****			
グループY	ユーザーE	*****	key23a	key23b	4356
	ユーザーF	*****			
	ユーザーG	*****			
	ユーザーH	*****			

【図7】

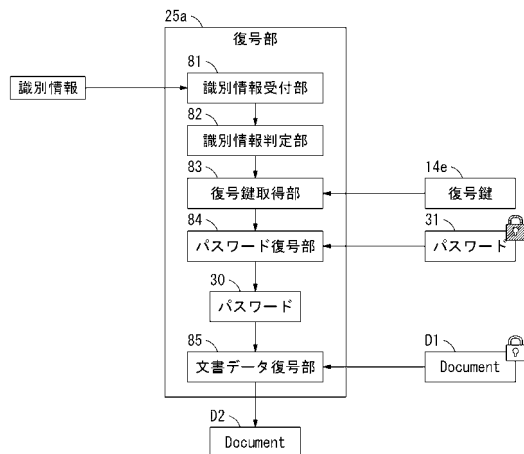
管理情報 35

35a	35b	35c	35d
グループ	共有文書ファイル名	アップロードユーザー	パスワード情報
グループX	Document001.pdf	ユーザーA	*****
	Document002.pdf	ユーザーA	*****
	Document003.doc	ユーザーB	*****
グループY	Document111.pdf	ユーザーF	*****
	Document112.pdf	ユーザーE	*****
	Document113.doc	ユーザーH	*****

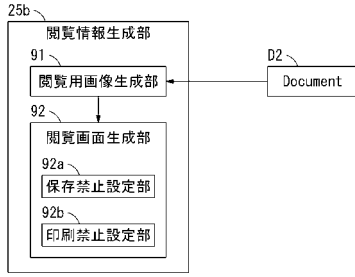
【図6】



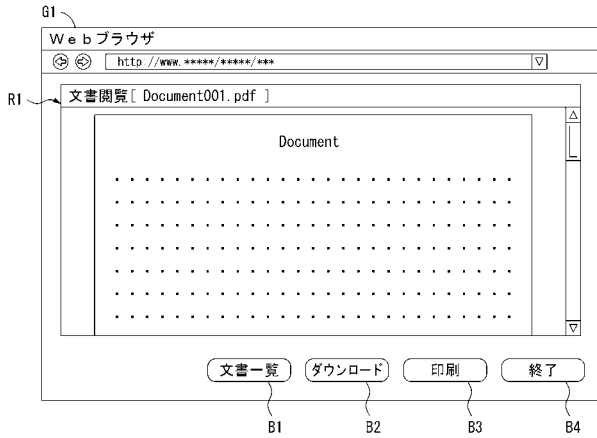
【図8】



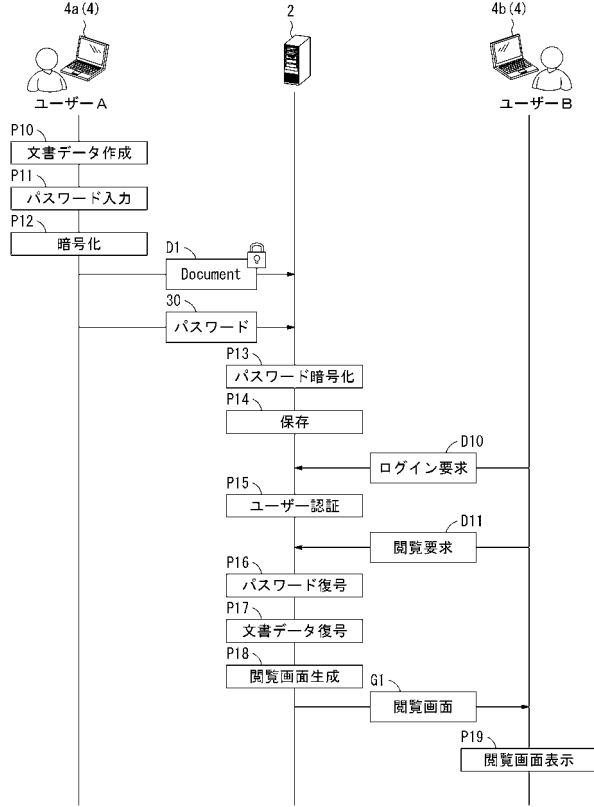
【図9】



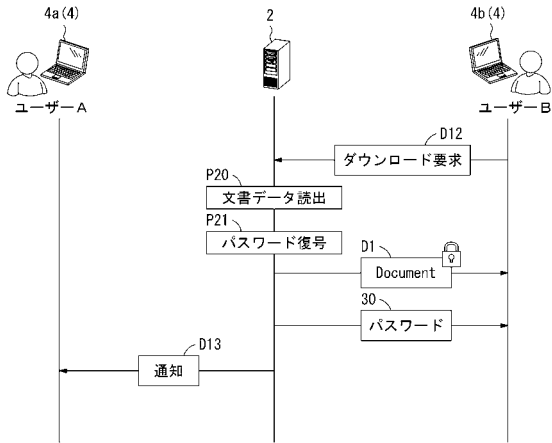
【図10】



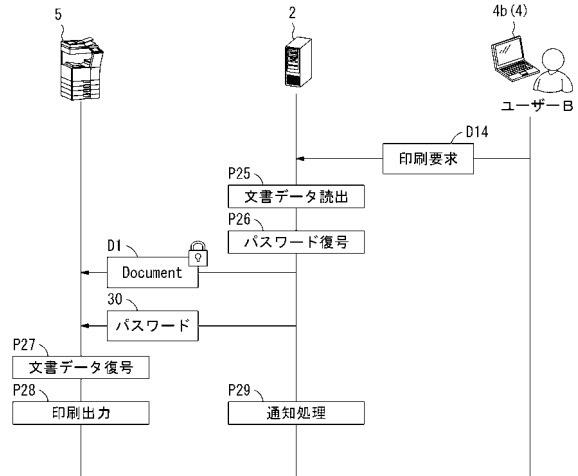
【図11】



【図12】

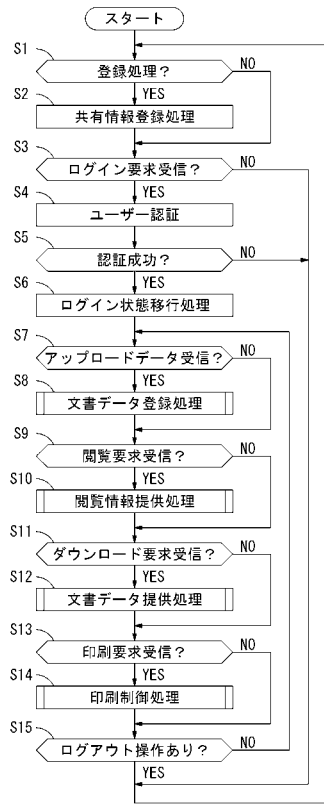


【図13】

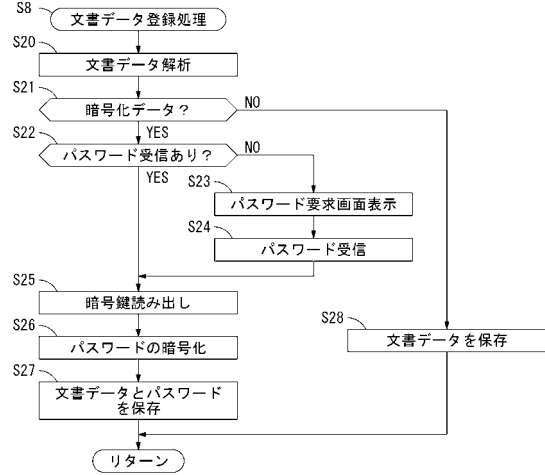


【 図 1 4 】

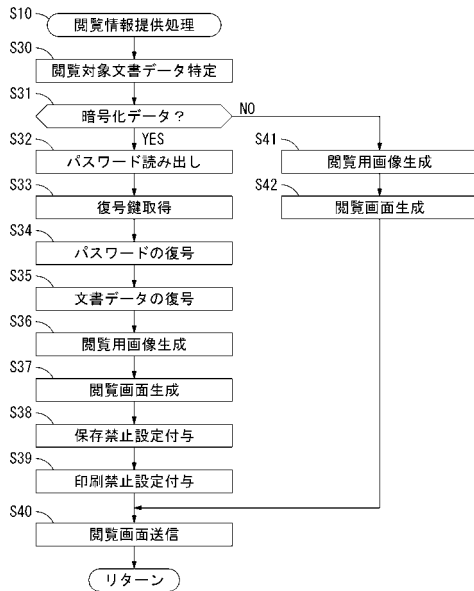
情報共有サーバ 2



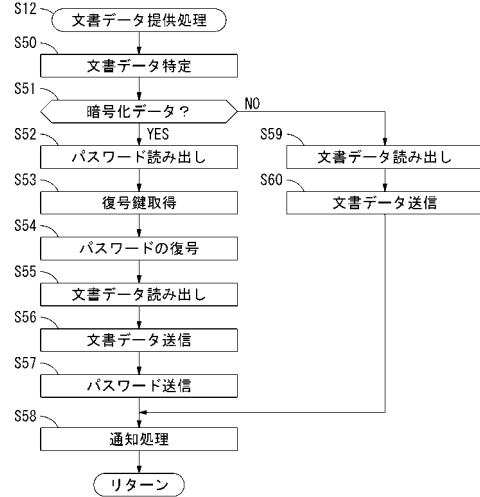
【 図 1 5 】



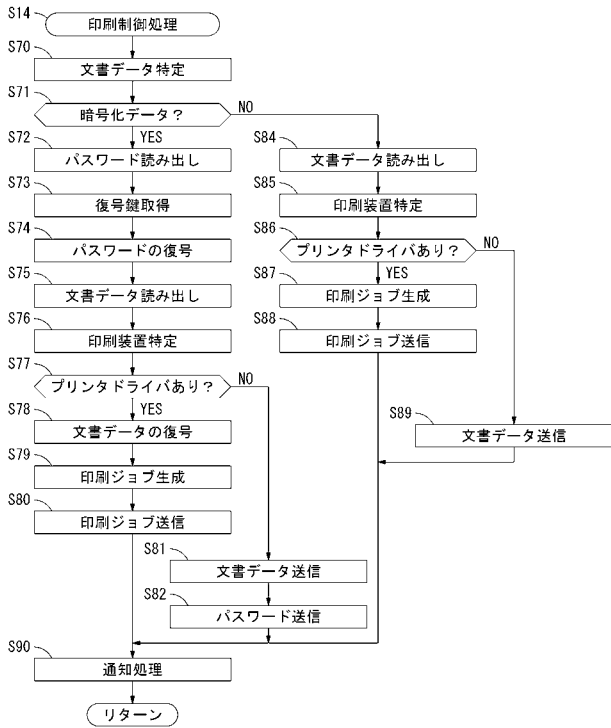
【 図 1 6 】



【 図 1 7 】



【図 18】



【図 19】

